VIGILÀNCIA MASSIVA AL MAGHREB I EL MASHREQ

Una anàlisi crítica per protegir l'espai de la societat civil

---

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

VIGILÀNCIA MASSIVA AL MAGHREB I EL MASHREQ

Una anàlisi crítica per protegir l'espai de la societat civil

Novembre 2024

Autores principals: Dúnia Camps-Febrer, Felip Daza, Carlos Díaz i Nora Miralles

Autores contribuents: Berta Flores i Paula Mas

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

Comunicació: Lucrecia Baquero Ramos (Observatori de Drets Humans i Empreses al Mediterrani), Julia Ponti Estrems (NOVACT), Ionan Areses (SUDS)

Assistència legal: Laia Serra Perelló

Maquetació: Carmela Márquez B @edicionescaseras

Traducció: Lia Giralt i Jorge Mills

L'Observatori de Drets Humans i Empreses al Mediterrani (DHE) és una iniciativa conjunta de SUDS i NOVACT

Agraïm a una sèrie de persones haver ofert generosament la seva ajuda: Itxaso Domínguez de Olazábal, Ahmed Ali, Omar Alaameri, Anabel Karina Arias, així com a totes les defensores de drets humans que han contribuït en la recerca i a tot l'equip de SUDS i NOVACT.

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

Informe realitzat en el marc del projecte:
Alhimaya – Defensa de l'espai cívic i protecció de defensores a l'Euromediterrània.

Amb el suport de:

Agència Catalana de Cooperació al Desenvolupament · Generalitat de Catalunya

ÍNDEX

ACLARIMENTS SOBRE LA TERMINOLOGIA UTILITZADA:

El dret internacional considera el territori palestí de Cisjordània, incloent-hi Jerusalem Est, i la Franja de Gaza, territori ocupat il·legalment per Israel. Altres autores consideren que tota la Palestina històrica (el territori colonitzat sota el protectorat britànic entre el 1918 i el 1948) està ocupada, ja que la creació de l'Estat d'Israel es va crear a partir de l'expulsió de gran part de la població autòctona que hi vivia, el poble palestí. En aquest informe, quan parlem de Territori Ocupat palestí (TOP), ens referim a la Franja de Gaza, Jerusalem Est i Cisjordània.

Les Nacions Unides consideren el Sàhara Occidental com un territori no autònom, el procés de descolonització del qual està subjecte al referèndum d'autodeterminació previst pel Pla de Pau de 1991. En aquest context, Espanya és la potència administradora, mentre que el Marroc es considera potència ocupant. Per a la Unió Africana i més de mig centenar d'Estats més, el Sàhara Occidental és la República Àrab Sahrauí, Democràtica un estat sobirà. En aquest informe, quan parlem de territori ocupat del Sàhara Occidental, ens referim a la República Àrab Sahrauí Democràtica.

A més, en aquest informe, en general, emprarem el femení genèric com a expressió lingüística referida a persones.

PRÒLEG

L'ús indiscriminat de la vigilància massiva per part d'Estats i empreses està posant en perill els fonaments de les democràcies a escala global.

Les noves tecnologies proporcionen als Governs eines cada vegada més potents per controlar els moviments socials, els mitjans de comunicació i la dissidència, en general. El sector tecnològic i el comerç de la vigilància actuen en un context pràcticament lliure de regulacions, convertint-se en una peça clau de l'arquitectura repressiva. Això ha portat a normalitzar pràctiques il·legals per part d'alguns Estats, que utilitzen aquestes eines per perpetuar el control i la repressió. És en aquest context on irromp la intel·ligència artificial i eleva encara més les dinàmiques de discriminació. A més, les regulacions que es creen no tenen enfocament extraterritorial i es salvaguarden en la seguretat nacional per tal d'incorporar-hi excepcions. Al setembre del 2021, l'Alta Comissionada de les Nacions Unides per als Drets Humans va demanar una "moratòria urgent en la venda i l'ús de la intel·ligència artificial" i les tecnologies associades. Segons el Relator de les Nacions Unides per a la Llibertat d'Expressió, la implementació de mecanismes de vigilància i control està afectant el dret a la llibertat d'expressió, opinió i privacitat, amb profundes vulneracions cap a les persones defensores de drets humans i periodistes.

Els mecanismes de vigilància i control erosionen greument drets fonamentals com la llibertat d'expressió, d'opinió i de privacitat, amb un impacte especialment dur sobre les persones defensores de drets humans i les periodistes, sovint objectiu directe d'aquestes pràctiques de persecució.

Aquest informe és una continuació del nostre estudi "Mass surveillance i control de la dissidència a Europa" (2021), on ja alertàvem sobre l'ús d'aquestes tecnologies per part de Governs europeus. Ara ampliem la nostra mirada cap al Maghreb i al Mashreq, dues regions on hi ha un patró clar: empreses del Nord Global —majoritàriament europees, nord-americanes i israelianes— desenvolupen tecnologia, sovint "testada en combat", en contextos de greus vulneracions de drets humans, especialment en territoris ocupats. Posteriorment, aquesta tecnologia és adquirida per règims cada vegada més autoritaris, amb l'objectiu de reprimir les dissidències i els moviments socials. Així, l'ascens de l'autoritarisme està sustentat per un entramat d'organitzacions, empreses i institucions que legitimen un ordre social d'opressió, basat en l'abús del poder estatal i empresarial, la polarització social i l'ús de la violència en les seves diverses formes.

Des del Marroc fins a l'Iraq, els Governs i les empreses privades de la regió estan desplegant eines de vigilància digital cada cop més sofisticades per identificar, monitorar i silenciar les dissidències, les periodistes, les defensores de drets humans i les activistes feministes i mediambientals. Molts d'aquests Governs compten amb el suport del nord global, qui avala aquestes pràctiques repressives amb l'objectiu de sufocar qualsevol amenaça a l'statu quo. Així doncs, existeix una interdependència en el desenvolupament i ús de les tecnologies de vigilància, que se sosté en un context global d'impunitat empresarial, que aquest

informe vol visibilitzar, amb l'objectiu d'identificar i comprendre les tendències que l'autoritarisme posa en pràctica en l'àmbit global, però també les seves especificitats en l'àmbit local.

Actualment, la regió mediterrània experimenta una severa limitació de l'espai cívic, indispensable per a l'exercici i la defensa de drets fonamentals com la llibertat d'expressió, d'associació i de reunió. Aquests drets són crucials per garantir una interacció lliure i segura entre la societat civil i els Governs, sense por de represàlies. Atenent la manera en què la tecnologia està generant les capacitats per tenir sota control a la dissidència, ens inquieta quin futur tenen les democràcies. Els drets que s'han aconseguit al llarg de la història no han estat concedits, sinó conquistats gràcies a les lluites socials. És altament preocupant que els Estats tinguin cada vegada més eines per monitorar, perseguir i silenciar els moviments socials i de defensa de drets humans, posant així en risc molts dels drets que tant han costat d'aconseguir.

Aquesta degradació democràtica restringeix la capacitat de la societat civil per autoorganitzar-se, implicar-se en la vida pública i erigir-se com a defensora de drets humans, amb un impacte especialment greu sobre aquells col·lectius més vulnerabilitzats per sistemes d'opressió basats en categories racistes, de gènere i de classe social.

És en aquest context que expressem la nostra preocupació sobre com les noves tecnologies estan reforçant aquestes desigualtats i faciliten la vulneració sistemàtica de drets i silencien les dissidències que lluiten contra aquesta deriva autoritària.

En aquest informe, aportem anàlisis i diagnosis d'allò que està passant i coneixement del fenomen i els matisos que s'adquireixen en diferents contextos, amb l'objectiu de construir estratègiques col·lectives per revertir-lo. També aportem arguments i eines per subratllar la necessitat urgent de regular aquestes tecnologies, que no només debiliten les democràcies, sinó que també posen en perill la vida de les persones i els col·lectius que treballen per defensar-les. La manca de mecanismes internacionals de regulació dificulta que les víctimes de la vigilància selectiva trobin justícia, reparació i garanties de no repetició. La creació de sistemes de control i regulació és imprescindible tant a escala estatal com supraestatal, tant per a les empreses que desenvolupen aquestes tecnologies com per a aquelles que les implementen i compren. En aquest sentit, volem alertar les administracions de la necessitat urgent d'establir mecanismes de control i seguiment que impedeixin la contractació pública d'empreses i compra de tecnologia vinculada a la vulneració de drets humans, en tota la cadena de subministrament. És urgent recordar als Estats i a les empreses que és la seva responsabilitat vetllar pel respecte dels drets humans i aquest informe és un pas més en aquesta direcció.

No volem acabar sense fer esment de la importància de la crear xarxes i estratègies de defensa de drets humans nord-sud que ampliïn les perspectives locals, en un intercanvi internacional basat en la reciprocitat. La interconnexió, l'intercanvi d'experiències i la creació d'aliances són el motor de canvi i transformació per a les entitats que promovem aquesta recerca.

INTRODUCCIÓ

Les tecnologies de vigilància i control, enteses com el maquinari i el programari necessari per monitorar el comportament, les activitats i la informació de la població, s'han convertit en un negoci lucratiu que l'any 2022 ja facturava més de 130 000 milions de dòlars i es calcula que actualment ja supera els 150 000 milions, a escala global.[1] És un mercat controlat fonamentalment per empreses occidentals, principalment israelianes, centreeuropees, i estatunidenques, els productes i tecnologies de les quals s'apliquen de manera profusa i cada vegada més estesa als països del Sud Global, tal com es mostra en aquest informe.

Aquest desenvolupament i aquesta inversió multimilionària en eines d'intel·ligència artificial i tecnologies digitals per al control social succeeix en un context global d'auge de l'autoritarisme, del militarisme i de les vulneracions de drets humans, en plena crisi ecològica i econòmica mundial de conseqüències encara incertes. Aquesta és una perspectiva que comparteixen bona part de les organitzacions de defensa dels drets humans i la democràcia al món. Amnistia Internacional advertia l'any 2019 que "aquest viratge autoritari global és existencial i amenaça a cada ésser humà i a totes les nostres llibertats, la igualtat i la justícia".[2]

No obstant això, l'ús i l'accés de les tecnologies digitals també és diferenciat, en funció de les característiques de la població i destaca aspectes com ara l'edat, el gènere o la divisió urbana-rural.[3] Tots aquests factors determinen l'impacte de les tecnologies digitals, tant com a via d'accés o producció d'informació diversa, com a via de control o repressió.

En el cas de la regió mediterrània, i més concretament al Maghreb i al Mashreq, des de les primaveres àrabs, els règims han invertit en tecnologies de vigilància massiva per controlar la dissidència política. Així i tot, el cas més extrem és l'ús que Israel fa del Territori Ocupat Palestí (TOP) com a laboratori d'assaig de noves armes i tecnologies sobre la població civil, fet que els ha permès ser líders mundials en exportació de tecnologies de repressió i control social, dinàmica que s'ha agreujat enormement des del 7 d'octubre del 2023. Des de l'inici del genocidi a Gaza, en un context on s'han desplegat sistemes d'intel·ligència artificial extremadament letals, més de 41 000 persones palestines han estat assassinades a mans de l'exèrcit israelià.

Aquests atacs a Gaza han potenciat l'ús i abús de la vigilància, no només contra la població palestina al TOP, sinó també contra la societat civil, que s'ha alçat a tot el món per denunciar

---

1 **Statista.com.** "Surveillance Technology Market Size Worldwide from 2022 to 2027." Disponible a: 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.** Reflexió: "The Global Authoritarian Turn: Making Humanity Win." 2019. Disponible a: https://amnesty.no/sites/default/files/vedlegg/the_global_authoritarian_turn_-_making_humanity_win.pdf

3 Veure dades desglossades per país a l'Arab Barometer: **Arab Barometer**. "The MENA Digital Divide." Disponible a: https://www.arabbarometer.org/2020/09/the-mena-digital-divide/

les massacres i la inacció de la comunitat internacional. A tot això s'hi suma la desconnexió digital forçada de la població libanesa als pobles i els suburbis on la infraestructura de comunicacions ha estat bombardejada i destruïda recentment per Israel. A les zones atacades, s'hi han documentat també missatges intimidatoris i falses crides d'evacuació, a través de les xarxes i les aplicacions de missatgeria per confondre, intimidar i espantar la població libanesa. Aquestes són tendències que sens dubte deixen intuir un augment del viratge autoritari global que requereix una anàlisi pròpia i urgent.[4]

En aquest informe, s'analitzaran les tendències i el caire que els darrers anys ha pres la vigilància massiva al Maghreb i al Mashreq, en continuïtat amb el projecte d'investigació "Vigilància hi-tech en temps de la COVID 19-19"[5] publicat per l'ODHE l'any 2021, que ja deixava entreveure algunes d'aquestes tendències i empreses. El nostre objectiu és contribuir a comprendre la incidència en la vulneració dels drets humans que té la relació entre els Governs i el sector empresarial, quan es despleguen les polítiques de seguretat interna. La investigació sobre casos i productes s'ha complementat amb entrevistes a defensores de drets humans que, en alguns casos, van participar en la trobada "The Nonviolence Factory" que va organitzar NOVACT i que es va celebrar a Barcelona el 2023, així com al "Seminari Al-Himaya en defensa i protecció de l'espai cívic davant la vigilància massiva a l'Euromediterrània", organitzat per SUDS, NOVACT i Iridia el maig del 2024.

Per això, és essencial comprendre com s'han desenvolupat i com s'han provat aquestes tecnologies i les implicacions socials i polítiques de l'ús d'aquestes eines, des d'una perspectiva dels drets humans. Desemmascarar la cadena global de la repressió i el control social amb un enfocament interseccional pot servir per reforçar la protecció, mobilització i feina de comunicació i incidència dels grups i col·lectius afectats per aquestes vulneracions, així com establir aliances entre defensores de drets humans de diferents territoris.

Conscients que la nostra posició i eines estan situades a Barcelona, hem adoptat una perspectiva decolonial, antiracista i feminista. És per això que la metodologia emprada incorpora el coneixement i l'experiència de les organitzacions i de les defensores de drets humans que hem entrevistat als diferents països del Maghreb i el Mashreq.

Hi ha una interdependència tecnològica en què el Nord Global extreu les matèries primeres dels països del Sud Global per fabricar tecnologies que s'assagen sobre les poblacions d'aquests països i que després s'utilitzen per perfeccionar la vigilància sobre les defensores de drets humans, periodistes, oposició política, dissidents de gènere i sexuals o persones migrants a tot el món.

Considerem que aquest context ens obliga a identificar i conèixer les implicacions que té la vigilància massiva en els drets humans i en les persones defensores de tota la regió mediterrània i d'aquesta manera, assumir la responsabilitat que tenim des del Nord Global.

---

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

5 **ODHE.** "Mass Surveillance." Disponible a: https://mass-surveillance.odhe.cat/

I

EL MARROC: EL PANÒPTIC ALAUITA

La vigilància digital al Marroc s'aplica sobretot a periodistes independents, persones defensores de drets humans i sobre la població sahrauí (vegeu capítol Sàhara Occidental). La repressió de les persones dissidents amb visibilitat és una estratègia molt efectiva, ja que reforça la sensació de control total sobre la resta de la població, que recorre a l'autocensura per evitar la repressió. El Marroc, a més, exerceix violència sobre persones d'interès fora del país (des de presidents i caps d'Estat, fins a periodistes estrangers). L'aparent arbitrarietat ha format sempre part de l'estratègia repressiva del règim. Per una banda, la persecució de grans figures mostra que no hi ha cap perfil d'alt nivell que estigui protegit i, per altra banda, la repressió de la població anònima estén la idea del control total: el panòptic alauita.[6]

"La repressió de les persones dissidents amb visibilitat és una estratègia molt efectiva, ja que reforça la sensació de control total sobre la resta de la població, que recorre a l'autocensura per evitar la repressió"

Els atemptats de Casablanca de l'any 2023 van accelerar l'entrada del Marroc al marc de lluita antiterrorista promogut pels Estats Units.[7] La llei antiterrorista del 2023, polèmica, però aprovada per unanimitat després dels atemptats va donar carta blanca per monitorar els mitjans de comunicació i els continguts d'alguns llocs web, blogs i altres espais. Es van detenir i empresonar milers de persones sense càrrecs durant dies[8] i es van vigilar organitzacions, moviments i defensores de drets humans crítiques amb el règim, sota el pretext lax de la 'seguretat nacional' i 'l'ordre públic'.[9]

6 La primera detenció per contingut personal en línia que es coneix va ser el febrer del 2008. Agents de paisà van detenir Fouad Mourtada per haver creat un perfil fals del germà del rei i aquesta detenció va destapar la possible vigilància massiva en línia. Fouad no era cap activista conegut.

7 De fet, la col·laboració amb els Estats Units en la seva "guerra contra el terror" ja havia començat abans del 2003. El Marroc va ser un dels països que va aportar *black sites* (nom amb què es denominen els centres clandestins de detenció operats per la CIA, generalment ubicats fora del territori continental dels estats units i la seva jurisdicció) per segrestar i torturar presoners de la CIA, després dels atemptats del 2001. **Tom Finn**. "How Arab states helped the CIA with its torture-linked rendition program." Middle East Eye, 13 de febrer del 2015.
Disponible a:
https://www.middleeasteye.net/news/how-arab-states-helped-cia-its-torture-linked-rendition-program

8 La llei antiterrorista del 2003 permet, a més, mantenir una persona detinguda fins a 12 dies, sense passar a disposició judicial. **Human Rights Watch**. "Stop Looking for Your Son. Illegal Detentions under the Counterterrorism Law." 25 d'octubre del 2010.
Disponible a:
https://www.hrw.org/report/2010/10/25/morocco-stop-looking-your-son/illegal-detentions-under-counterterrorism-law

9 A més, els delictes d'opinió contra la monarquia, la religió i la 'sobirania nacional' poden arribar a comportar fins a sis anys de presó. **Departament d'Estat, EUA**. "Morocco 2023 Human Rights Report."
Disponible a:
https://www.state.gov/wp-content/uploads/2024/02/528267_MOROCCO-2023-HUMAN-RIGHTS-REPORT.pdf

Des de principis dels 2000, el Marroc ha anat adoptant lleis per controlar l'esfera digital (Llei de Ciberdelinqüència el 2023, Llei de Ciberseguretat el 2020).[10] El setembre del 2011 es va crear la Direcció General de Seguretat dels Sistemes d'Informació[11] i el maCERT, el "centre de vigilància, detenció i resposta als atacs informàtics". Tant la Direcció General com el maCERT estan sota la direcció de l'Administració de Defensa Nacional[12], que equival al Ministeri de Defensa. Això vol dir que una part de la infraestructura de control no s'ha creat sota el paraigua del Ministeri de l'Interior o d'Informació, sinó dins d'una institució militar, on no hi ha rendició de comptes ni transparència.[13]

Tot i que, segons Freedom House, el Marroc és 'parcialment lliure'[14], en l'àmbit de l'accés i les llibertats a internet, l'adopció de lleis de premsa i de llibertats amb estàndards més o menys acceptables amaga un ús pernicios del sistema judicial i del Codi Penal.[15] La majoria de defensores de drets humans i periodistes no han estat acusades i condemnades sota la Llei de premsa i publicacions, sinó en el marc de delictes tipificats al Codi Penal, que comporten penes de presó. Aquí es conjuguen, doncs, una legislació repressiva, la connivència necessària del sistema judicial i una xarxa de tecnologies intrusives, moltes d'elles desenvolupades per emprses europees.

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

11 La Direcció General de Seguretat de Sistemes d'Informació va ser creada pel decret 2-11-509 del 21 de setembre del 2011. Es una administració adjunta a l'Administració de Defensa Nacional.

12 Hassan II va abolir el Ministeri de Defensa l'any 1972. Actualment, l'Administració de Defensa Nacional depèn directament del Rei, a través del ministre delegat de l'ADN, també ministre de l'Interior, Abdellatif Loudiyi.

13 **Freedom House**, "Freedom on the Net 2023: Morocco," accés 12 de setembre del 2024.
Disponible a: https://freedomhouse.org/country/morocco/freedom-net/2023

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

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

1. LES XARXES SOCIALS, MOBILITZACIÓ I POR A PERDRE EL CONTROL DEL RELAT

L'augment de l'ús de les xarxes socials va suposar un problema pel règim que, amb casos com el de l'*sniper* de Targuist o franctirador de Targuist[16] [17], des del 2007, veia com la població podia denunciar el sistema pel seu compte. Amb tot, el principal punt d'inflexió en la vigilància digital va ser durant les revoltes del 2011 i el Moviment del 20 de febrer.[18] El gran poder de mobilització de la societat civil en les revoltes del 2011 que es va estendre per la regió es va dur a terme a través d'internet, en concret a través de Facebook i Youtube. És el cas de la campanya *Mamfakinch*, organitzada per un col·lectiu social dies abans de les primeres protestes del febrer.[19] [20]

De fet, una de les primeres compres marroquines pel control digital que es van conèixer va ser la del *malware*[21] en forma de troià[22] d'activació remota a la tecnològica italiana Hacking Team. Es va fer servir contra periodistes i contra la campanya Mamfakinch.[23] Entre els clients hi havia dues agències d'intel·ligència marroquines (el Consell Superior de la Defensa Nacional – CSDN i la Direcció General de Vigilància Territorial – DST), que van obtenir el programari els anys 2009 i 2012 respectivament.[24]

16 **Jeune Afrique**, "Corruption au Maroc : le « sniper de Targuist » poursuit son combat à visage découvert," 4 de març del 2013. Disponible a: 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 a: https://www.youtube.com/watch?v=l9IVKf5Hk4Q

18 Moviment de masses, les demandes polítiques del qual incloïen la reforma del sistema polític 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 a: https://www.academia.edu/34822277/Under_watchful_eyes_Internet_surveillance_and_citizen_media_in_Morocco_the_case_of_Mamfakinch

20 Tot i la repressió, hi ha hagut diverses campanyes de mobilització a internet amb un gran impacte, com la del setembre del 2018, #Masaktach ("NoCallaré") contra la violència masclista i l'assetjament sexual; o la campanya de boicot, el mateix any, contra diverses empreses, estretament lligades al règim (Central Danone, Sidi Ali, Afriquia). **Freedom House**. "Freedom on the Net 2019." Disponible a: https://freedomhouse.org/country/morocco/

21 Vegeu glossari

22 Vegeu glossari

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

24 Ibid.

L'octubre del 2016, es van iniciar les protestes massives de Hirak Rif (Moviment Popular del Rif), que durant setmanes, va congregar milers de persones a Al-Hoceima i d'altres poblacions del nord del Marroc. A més de la repressió in situ, entre el maig i l'agost del 2017, hi va haver defensores de drets humans, periodistes o blogueres que van ser detingudes per les seves activitats a internet.[25] [26]

2. LA MANIPULACIÓ DE LES XARXES SOCIALS

Actualment, les xarxes socials són la principal font d'informació de la població marroquina, amb Youtube i Facebook al capdavant,[27] ja que són les úniques formes de comunicació que se surten del discurs oficial. Per tant, aquestes són les xarxes en les quals se centra el control i la repressió, que es duen a terme amb diferents tipus d'estratègies.

Una d'elles ha estat la utilització de les xarxes de comportament inautèntic coordinat,[28] que buscaven influir en l'opinió pública a escala local i regional. Meta va eliminar centenars de comptes de Facebook i Instagram vinculats a activitats progovernamentals que elogiaven la gestió del Govern del Marroc de la pandèmia, les seves iniciatives diplomàtiques i la resposta de les forces de seguretat, a més d'alabar el rei Mohammed VI i alguns alts funcionaris de seguretat.[29] [30] Els comptes estaven relacionats amb mitjans pro-règim com ChoufTV, coneguda per la seva tasca difamatòria contra defensores dels drets humans.[31] Segons Meta, vora 150 000 comptes seguien a una o més d'una d'aquestes pàgines.

---

25 Activistes pacífics com Nasser Zefzafi i El Mortada Iamrachen van ser acusats de 'trencar el respecte al rei', 'ofendre les institucions constitucionals' o 'insultar càrrecs públics'. Rabieh Al-Ablaq va ser sentenciat el juny del 2017 a 5 anys de presó per 'publicació de notícies falses' i 'usurpació del títol de periodista'. Al-Ablaq va denunciar les tortures patides durant els interrogatoris de la política a Alhuceimas.

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

27 Així i tot, hi ha diferències substancials entre l'accés a internet i el seu ús per part de dones i homes, entre la població rural i urbana i entre joves o persones més grans de 30 anys. **Arab Barometer.** "The MENA Digital Divide," setembre del 2020.
Disponible a: https://www.arabbarometer.org/2020/09/the-mena-digital-divide/

28 Vegeu glossari

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

30 Només el mes de febrer del 2021, es van eliminar 385 comptes i 6 pàgines de Facebook, així com 40 comptes d'Instagram operats des del Marroc i dirigides al públic general. Aquesta xarxa de comptes va ser desmantellada per Meta, després de les denúncies d'Amnistia Internacional. Facebook, "February 2021 CIB Report,". Març del 2021.
Disponible a: https://about.fb.com/wp-content/uploads/2021/03/February-2021-CIB-Report.pdf

31 **ADN (per les seves sigles en francès)**, "Defamation Campaign against Human Rights Defender Karima Nadir," Frontline Defenders.
Disponible a: https://www.frontlinedefenders.org/en/case/defamation-campaign-against-woman-human-rights-defender-karima-nadir

3. VIGILÀNCIA I CONTROL MASSIU DE LES COMUNICACIONS

La vigilància i el control massiu de les comunicacions es du a terme amb l'ajuda de tecnologies punteres. Això implica un control de la informació que circula i es publica, però també apagades digitals puntuals.[32] Tot i que el filtratge (bloqueig de determinades pàgines i informacions) no és una de les eines més emprades, se segueix utilitzant de manera arbitrària i sense avís oficial.[33] Destaquen els mecanismes de vigilància especialment intrusius contra les defensores de drets humans i les persones crítiques amb el règim.

El 2019, Amnistia Internacional va denunciar que els dispositius de destacades defensores de drets humans havien estat infectats amb Pegasus, com ara, el de l'activista sahrauí Aminatou Haidar, el de l'historiador Maati Monjib, els dels periodistes i investigadors Taoufik Bouachrine, Omar Radi, Soulaimane Raissouni o el de l'advocat de drets humans Abdessadak El Bouchattaoui. Segons aquests periodistes, alguns dels continguts i materials que es van obtenir amb Pegasus es van fer servir per difamar-los, fer-los xantatge i assetjar-los.

L'any 2022, Amnisitia Internacional i Citizen Lab van trobar proves sòlides de l'ús d'aquest programari espia[34] Pegasus, de l'empresa israeliana NSO Group, per part de les autoritats del Marroc i es va fer una llista de possibles afectades, amb fins a 10 000 persones, incloent-hi el mateix rei Mohammed VI.[35] [36] El Marroc també va espiar defensores de drets humans sahrauís i figures prominents a l'estranger, com ara periodistes franceses i el president Emmanuel Macron i a Espanya, el president del Govern, Pedro Sánchez, i la ministra de Defensa i els ministres d'Interior i Agricultura. Tot i que NSO ha negat la utilització del seu programari en aquests casos, no ha publicat els resultats d'una investigació que va prometre que es faria el 2019. A més, el Ministeri de l'Interior del Marroc també hauria

32 Del 25 al 30 de maig del 2007, YouTube va ser bloquejat per la principal empresa de telecomunicacions,: Maroc Telecom (les altres dues, Wana i Meditel, no el van bloquejar). **Global Voices**, "Morocco Blocks Access to Youtube,". 26 de maig del 2007.
Disponible a: https://globalvoices.org/2007/05/26/morocco-blocks-access-to-youtube/

33 El gener del 2016, Maroc Telecom, Meditel i Inwi van bloquejar trucades a través d'internet (VoIP) amb 3G i 4G (Skype, Viber, Tango, WhatsApp i Facebook Messenger, entre d'altres). **Saad Guerraoui**, "Morocco banned Skype, Viber, WhatsApp and Facebook Messenger. It didn't go down well," **Middle East Eye**. 9 de març del 2016.
Disponible a:
https://www.middleeasteye.net/opinion/morocco-banned-skype-viber-whatsapp-and-facebook-messenger-it-didnt-go-down-well

34 Vegeu glossari

35 **Forbidden Stories.** "About the Pegasus Project." Forbidden Stories. 18 de juliol del 2021.
Disponible a: 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 juliol del 2021.
https://elpais.com/internacional/2021-07-20/macron-en-el-punto-de-mira-del-programa-de-espionaje-pegasus-contratado-por-marruecos.html

estat client[37] de Circles Technologies, com a mínim des del 2018 i feia servir un sistema d'aquesta empresa, afiliada al grup NSO Group, per controlar trucades, missatges de text i ubicacions, a partir de vulnerabilitats de les xarxes.

Per altra banda, el grup de periodisme d'investigació francès Reflet va destapar la compra d'Eagle System per part del Marroc,[38] un sistema de vigilància digital massiva del trànsit d'internet, amb funcions de censura (a través de Deep Packet Inspection[39]), propietat de l'empresa francesa Amesys (Nexa Technologies). L'any 2011, el Marroc havia invertit prop de 2 milions d'Euros en el sistema Eagle, desenvolupat sota el nom de "Project Popcorn".[40]

La investigació de l'organització Citizen Lab també va destapar la compra del programari maliciós[41] FINFIsher[42] per part de Consell Superior de la Defensa Nacional del Marroc.[43] FINFIsher (o Finspy), de l'empresa angloamericana Gamma Group, es ven exclusivament a agències governamentals i forces policials, a través de Lench IT Solutions plc. El programari controla de manera remota qualsevol aparell infectat prèviament i pot copiar arxius, interceptar trucades d'Skype i inclús registrar els moviments del teclat.

37 **Citizen Lab.** "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." Citizen Lab, 2020. Disponible a: 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 a: https://privacyinternational.org/report/1125/their-eyes-me-stories-surveillance-morocco

39 Vegeu glossari

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

41 Vegeu glossari

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 d'octubre del 2015. Disponible a: 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 d'octubre del 2015. Disponible a: https://www.zdnet.com/article/in-hacking-teams-wake-finfisher-spyware-rises-in-popularity-with-government-users/

4. ASSETJAMENT EN LÍNIA: CAMPANYES DE DESPRESTIGI I EMBOSCADES DIGITALS44

En els atacs i troleig en línia[45] han destacat les campanyes de desprestigi, estratègia molt utilitzada al Marroc. Human Rights Watch ho anomena *character assassination campaigns* (campanyes d'assassinat del personatge), en les quals, de manera aparentment orquestrada, s'inicien campanyes de difamació i notícies falses.[46] Molt sovint, aquestes campanyes ataquen les llibertats sexuals de les defensores de drets humans. En un informe de Meta del desembre del 2021,[47] s'esmenta el Marroc com a origen de perfils de comptes de Facebook i Instagram vinculats al programari israelià Cognyte (antiga WebintPro). Aquest problema permet la creació i gestió de comptes falsos a xarxes socials com Facebook, Instagram, Twitter i Youtube i també recull dades d'aquestes xarxes. Segons el mateix informe de Meta, el seu objectiu apunta principalment a periodistes i polítiques.[48] A més, s'han identificat grups de hackers que actuen per sabotejar contingut crític a les xarxes o infiltrar-se a les xarxes socials o correus electrònics privats.[49]

"A les dones activistes, periodistes o personalitats públiques crítiques amb el govern se les ataca especialment amb violència masclista en línia, amb contínues campanyes de difamació sobre la seva llibertat sexual i amb assetjament."

44 Vegeu glossari

45 Vegeu glossari

46 **Human Rights Watch**, "'They'll Get You No Matter What': Morocco's Playbook to Crush Dissent," 28 de juliol del 2022. Disponible a:
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 desembre del 2021.
Disponible a:
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 desembre del 2021.
Disponible a:
https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

49 El setembre del 2013, la web Investigative Journalism al Marroc va ser piratejada i els continguts van ser substituïts per porno (una estratègia habitual). La plataforma independent d'informació Lakome.com va ser bloquejada judicialment el 17 d'octubre del 2013 i no s'ha pogut restablir. El seu director i periodista Ali Anouzla va ser detingut sota la Llei antiterrorista, per haver vinculat un article del país sobre AlQaeda. **Reporters Without Borders**, "Website editor held for posting Al Qaeda video," 20 de setembre del 2013.
Disponible a:
https://web.archive.org/web/20150610182747/http://en.rsf.org/morocco-website-editor-held-for-posting-19-09-2013,45197.html

A les dones activistes, periodistes o personalitats públiques crítiques amb el Govern se les ataca especialment amb violència masclista en línia, amb contínues campanyes de difamació sobre la seva llibertat sexual i amb assetjament.[50] ChoufTV va publicar el 2020 informació difamatòria de l'activista pels drets de les dones Karima Nadir.[51]

Human Rights Watch també denuncia els atacs de tipus entrampament digital[52] contra persones de la comunitat LGBTQIA+. L'any 2020, es va orquestrar una campanya homòfoba d'*outing*[53] forçat d'homes gais o bisexuals, a través d'aplicacions.[54] Les relacions sexuals entre persones del mateix sexe estan prohibides al Marroc i, a més de la persecució judicial, aquestes informacions poden tenir conseqüències socials greus per a les persones, com ara violència física directa, represàlies professionals, etc.

La repressió que es pateix en línia, té sovint tres conseqüències: autocensura, sexili[55] o repressió física. En el marc de les campanyes de difamació sexualitzades, el periodista Taoufik Bouachrine, director del diari *Akhbar al Yaum*, va ser condemnat l'any 2018 a 15 anys de presó per diversos delictes (tràfic de persones, agressió sexual, violació, prostitució i assetjament) després d'una agitada campanya mediàtica.[56] La seva companya, Hajar Raissouni, va ser detinguda el 2019 pels càrrecs "d'avortament il·legal" i "relacions sexuals fora del matrimoni" i per estar embarassada del seu cap.[57] Les autoritats marroquines van intentar provar els càrrecs tant si com no i inclús van obligar-la a sotmetre's a un examen mèdic sense el seu consentiment. La van condemnar a un any de presó abans que fos alliberada gràcies a un indult reial[58] i obligada a marxar del país.

---

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

51 Van ordenar la seva detenció, la van acusar de consum de drogues i mare soltera negligent. Karima Nadir és cofundadora del col·lectiu 490Collective i vicepresidenta de l'Associació pels Drets Digitals.

52 Vegeu glossari

53 Vegeu glossari

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

55 Fa referència a la situació en què les persones del col·lectiu LGBTIQ+ es veuen obligades a abandonar el seu lloc d'origen per causa de la discriminació, el rebuig i la violència a què s'enfronten per la seva orientació sexual o identitat de gènere.

56 L'organització Euro-Mediterranean Human Rights Monitor va identificar més de 30 pàgines i diaris online pro-règim que havien participat en campanyes d'aquestes característiques. **Reporters Without Borders**, "After long jail term, Moroccan journalist hit by heavy damages award," 7 de desembre del 2018.
Disponible a: 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 setembre del 2019.
Disponible a: https://www.hrw.org/news/2019/09/09/morocco-trial-over-private-life-allegations

58 El perdó reial es repeteix amb ocasió de festes nacionals importants. En aquestes ocasions, es publica una llista de 'perdons' que el Rei atorga a persones prèviament condemnades per la justícia. L'arbitrarietat del perdó reial és evident. L'any 2020 el perdó reial va incloure a membres del Moviment del Rif. L'any 2014 diversos periodistes de perfil alt van ser 'perdonats': Omar Radi, Souleimane Raussouni i Taoufik Bouachrine, Hicham Mansouri, Samad Ait Aicha, Imad Stitou, y Afaf Bernani.

II

EL SÀHARA OCCIDENTAL: VIGILÀNCIA PER MANTENIR L'OCUPACIÓ

Des que es va trencar la treva del 1991 entre el Front Polisario i el Marroc i, després de la incursió de les forces marroquines, el 13 de novembre del 2020 per expulsar un grup d'activistes sahrauís que protestaven per l'espoli de recursos del Sàhara Occidental ocupat pel Marroc, les hostilitats entre tots dos actors s'han identificat. Paral·lelament, també ha augmentat la repressió i la persecució de les organitzacions i defensores pro-sahrauís.

1. LA MODERNITZACIÓ DELS SISTEMES DE VIGILÀNCIA DEL MARROC

L'ocupació del Marroc del territori del Sàhara Occidental ha depès, en gran part, de la capacitat de controlar, vigilar, i reprimir a la població autòctona sahrauí. Des de l'any 2020, la situació dels drets humans al territori ocupat del Sàhara Occidental s'ha tornat més alarmant. La creixent digitalització en el panorama africà i marroquí ha influït en els mètodes, l'impacte i l'augment de les estratègies de vigilància sobre la població del Sàhara Occidental.[59] A més, l'acostament del Marroc a Israel, des del restabliment de relacions l'any 2020,[60] ha permès la seva col·laboració en la modernització i el desenvolupament d'instruments d'intel·ligència i vigilància. Paral·lelament, des de l'any 2009, s'identifiquen acords amb l'empresa espanyola Indra Sistemas S.A.. Indra va signar un contracte per 6,3 milions d'euros per instal·lar tres estacions que ampliaven la xarxa de vigilància per satèl·lit a les ciutats d'Al-Aaiun, Smara i Dajla.[61] El maig del 2024 Indra i l'Agència de Desenvolupament Digital (ADD) del Marroc van signar un acord destinat a accelerar el procés de transformació digital del Marroc.[62]

La vigilància de la població civil sahrauí per part de les autoritats marroquines s'ha basat en l'ús de la seva mà d'obra, la introducció d'informants i colons, el control de les fronteres, l'aïllament de la població i la persecució i repressió de la dissidència.[63] Les autoritats marroquines han estat sotmetent la població sahrauí a una vigilància constant, tant física

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 desembre del 2020. Disponible a: 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 desembre del 2020. Disponible a: 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 d'octubre del 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 maig del 2024. https://www.eleconomista.es/telecomunicaciones/noticias/12841197/05/24/indra-impulsara-la-transformacion-digital-de-marruecos.html

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

com tecnològica[64]; tal com informen mitjans com Per Un Sàhara Lliure (PUSL).[65] Altres fonts denuncien la instal·lació de càmeres de vigilància a Al-Aaiun, Smara, Dajla i fins i tot, a ciutats més petites del Sàhara Occidental ocupat pel Marroc.[66]

Els dos òrgans principals que duen a terme aquesta vigilància són les forces policials marroquines i el Direcció General de Vigilància Territorial (DGST, per les seves sigles en francès), l'òrgan governamental del servei d'intel·ligència civil del Marroc. Aquests dos òrgans de les forces marroquines[67] estan integrant noves tecnologies en les seves estratègies i mecanismes de control. Des del 2023, el DGST col·labora amb el *Federal Bureau of Investigation* (FBI) dels EUA en una aliança "antiterrorista" que aborda la zona "Sàhara-Sahel"[68] i que acaba facilitant el control sobre les dissidències al territori.

64 **Amnistia Internacional**, "Derechos Pisoteados: Protestas, Violencia y Represión en el Sáhara Occidental," 2010. Disponible a: 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 **Amnistia Internacional**, "Derechos Pisoteados: Protestas, Violencia y Represión en el Sáhara Occidental," 2010. Disponible a: 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 febrer del 2023. Disponible a:
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 VIGILÀNCIA INSTITUCIONAL A 'L'AUTOVIGILÀNCIA'

L'Estat marroquí va declarar l'estat d'emergència el 20 de març del 2020, amb l'objectiu de protegir la població de la pandèmia de COVID-19.[69] El 23 de març del 2020 es va aprovar l'estat d'emergència amb la Llei No. 2.20.292, que estableix penes i multes per a qualsevol persona que incompleixi "ordres i decisions de les autoritats" i per a qualsevol persona que "obstrueixi" aquestes decisions, incloent-hi la difusió "d'escrits, publicacions o fotos" a les xarxes socials.[70]

Pel que fa a la tecnologia, una de les principals iniciatives va ser el desenvolupament d'una aplicació mòbil per part d'enginyers i tècnics de la Direcció General de la Seguretat Nacional marroquina (DGSN) amb el suport del Ministeri de Sanitat i el Ministeri de l'Interior.[71] L'aplicació (app) Wiqaytna, és una eina voluntària per identificar a persones que hagin estat en contacte amb algú positiu per COVID-19. L'aplicació compleix amb la Llei Núm. 09-08, l'article 4 de la qual no obliga les autoritats a obtenir el consentiment d'una persona per processar les seves dades personals, quan es fan servir per a l'àmplia tasca de protegir l'interès públic, fer que permet un control massiu dels moviments de la població. Això permet un control massiu dels moviments de la població.[72]

Les autoritats marroquines van posar fi oficialment a l'estat d'emergència sanitària el febrer del 2023,[73] fet que va desactivar la Llei núm. 2.20.292, però s'ha pogut observar com l'estratègia d'autovigilància i censura poblacional s'ha traduït en altres polítiques de cibervigilància. El juny del 2024, la Direcció General de Seguretat Nacional va posar en funcionament la plataforma E-Blagh,[74] que permet a la societat civil denunciar ciberdelic-

69 **Europa Press Internacional**, "Marruecos declara el estado de emergencia desde este viernes y 'hasta nuevo aviso' por el coronavirus," 20 de març del 2020.
Disponible a:
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," presentat al Parlament del Regne del Marroc, 2020.
Disponible a: https://www.cg.gov.ma/fr/node/9696

71 **Access Now**, "COVID-19 Contact-Tracing Apps in MENA: A Privacy Nightmare". 18 de juny del 2020.
Disponible a: 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 febrer de 2024.
Disponible a:
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 juny del 2024.
Disponible a:
https://www.h24info.ma/e-blagh-la-plateforme-de-lutte-contre-la-cybercriminalite-desormais-operationnelle/

tes i notificar directament les autoritats d'alguna infracció o delicte digital, fet que, segons l'article 267-591 del Codi Penal marroquí, inclou "qualsevol amenaça a la integritat del regne del Marroc". El desenvolupament d'aquesta plataforma involucra a la població perquè denunciï i controli els ciberdelictes.[75]

3. EL CONTROL DELS MITJANS DE COMUNICACIÓ I LA PERSECUCIÓ DE PERIODISTES

El control dels mitjans de comunicació i la censura del periodisme han estat estratègies clau del Govern del Marroc per mantenir el control sobre el Sàhara Occidental i defensar-ne la legitimitat a nivell internacional.[76] Segons un informe de Reporters Sense Fronteres sobre les violacions contra el sector periodístic en aquest conflicte, "el periodisme és una de les moltes víctimes d'aquest conflicte oblidat pels mitjans, que ha convertit al Sàhara Occidental en un veritable 'forat informatiu'".[77] El desenvolupament digital ha afectat les periodistes sahrauís, a través de la persecució mitjançant mitjans digitals. Segons diu el periodista Ahmed Ettanji d'Equipe Media, "la repressió digital també és una qüestió molt important, perquè bona part de la nostra feina és digital i està basada en les xarxes socials i encara més, en els mitjans de comunicació alternatius".[78] Segons Ettanji, això té un "impacte individual en la limitació del moviment, perquè s'està vigilat, sigui de manera física o tecnològica" i no permet treballar "d'una manera lliure".[79]

A més, les dones periodistes pateixen una doble vulnerabilitat, com va ser el cas de la Nazha el Khalidi, que va ser interrogada i torturada per les forces policials del Marroc i a més, va patir difamació de caràcter masclista.[80] Seguint amb aquesta línia, segons l'informe

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

76 **Amnistia Internacional**, "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 **Reporters Sense Fronteres**, "Marruecos/Sáhara Occidental," Reporters Sense Fronteres.
Disponible a: https://rsf.org/es/pais/marruecos-sahara-occidental

78 Ahmed Ettanji, entrevista realitzada en el marc de The Nonviolence Factory, novembre del 2023. Equipo NOVACT, SUDS, IRIDIA y ODHE.

79 Ibid

80 **Reporters Sense Fronteres**, "Sáhara Occidental, un desierto para el periodismo," 2019.
Disponible a:
https://www.rsf-es.org/wp-content/uploads/attachments/2019_SAHARA_OCCIDENTAL_RSF_ES_INFORME.pdf

d'OpenNet Initiative del 2007,[81] el Marroc ha censurat nombroses webs, principalment, aquelles que donen suport a la independència del Sàhara Occidental, com ara la pàgina de la Unió de Periodistes i Escriptors Sahrauís.[82]

El Govern del Marroc fa servir principalment com a eina de persecució i control social a periodistes el programari espia[83] Pegasus, que pertany al grup israelià NSO Group. Segons Amnistia Internacional, aquesta tecnologia també s'ha fet servir per espiar defensores de drets humans sahrauís,[84] entre les quals hi ha la defensora de drets humans Aminatou Haidar.[85] Aquesta organització acredita que la falta de transparència a la indústria de la vigilància (per part d'empreses i Governs) dificulta poder saber quines eines s'estan venent, comprant i fent servir, fet que impedeix que les víctimes puguin exigir responsabilitats.

"La falta de transparència a la indústria de la vigilància (per part d'empreses i Governs) dificulta poder saber quines eines s'estan venent, comprant i fent servir, fet que impedeix que les víctimes puguin exigir responsabilitats"

Els programaris espia[86] s'utilitzen freqüentment per identificar periodistes dissidents, amb l'objectiu de silenciar la seva feina. A més, l'augment de la persecució contra periodistes sahrauís ha fet més difícil que es puguin documentar les violacions de drets humans al Sàhara Occidental, des de fora del territori. Un cas paradigmàtic d'assetjament va ser la repressió de la parella de defensores de drets humans sahrauí d'Equipe Media Ahmed Ettanji y Naziha El Khalidi, que van ser sotmeses a arrest domiciliari i inclús es va impedir el seu casament. Es creu que els atacs a periodistes sahrauís són una resposta directa als seus reportatges sobre la repressió actual

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

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

83 Vegeu glossari

84 **Amnistia Internacional**, "Morocco/Western Sahara: Activist Targeted with Pegasus Spyware in Recent Months – New Evidence," 22 d'octubre del 2023.
Disponible a:
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 març del 2016.
Disponible a:
https://www.middleeasteye.net/news/pegasus-spyware-morocco-western-sahara-activist-targeted

86 Vegeu glossari

al territori ocupat, una activitat que posa en risc la seva integritat física.[87] La persecució de periodistes sahrauís limita la seva llibertat de moviment i a més, els impedeix fer la seva feina lliurement. La persecució també afecta l'entorn familiar i la salut mental de les periodistes i genera un impacte econòmic i deteriora la cohesió social. A tot això cal afegir-hi que el factor gènere ha agreujat la vulnerabilitat de les dones periodistes i les ha exposat a més riscos i represàlies, tal com s'ha documentat en els casos de violència que han patit, per exemple, les defensores sahrauís Mbarka Mohamed al-Hafiz y Fatima Mohamed al-Hafiz.[88]

4. L'ÚS DE DRONS: CONTROLAR I ATACAR DES DE L'AIRE

Després que es trenqués l'alto el foc, l'any 2020, que va exacerbar les hostilitats al territori, el Marroc ha fet ús de la tecnologia de drons per establir el control sobre el territori. S'han fet servir per perpetrar atacs i també per vigilar les activitats al territori ocupat i als campaments de persones refugiades.[89] Els atacs de drons, suposadament estan dirigits a combatents del Front Polisario, però el seu ús ha afectat civils de diverses procedències i ha agreujat l'escalada del conflicte, més enllà del territori del Sàhara Occidental.[90] Per exemple, l'any 2021, un atac amb drons marroquins al Sàhara Occidental, controlat pel Front Polisari, va matar a tres camioners algerians.[91] Segons Africa Intelligence,[92] des del 2020, el Govern del Marroc ha integrat la tecnologia de drons per controlar els campaments sahrauís i les seves fronteres amb Algèria. Des de l'agreujament del conflicte, l'any

87 **NOMADS**, "Morocco/Western Sahara: First They Came for the Journalists. We Don't Know What Happened After That," 4 de desembre del 2020. Disponible a: 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 d'abril del 2022. Disponible a: 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 maig del 2023. Disponible a: 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 maig del 2024. Disponible a: 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

91 **Menadefense**, "Comprendre l'attaque marocaine contre les civils algériens". Disponible a: 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 desembre del 2021. Disponible a: 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

2021, el Govern marroquí ha signat un contracte amb l'empresa turca Baykar per adquirir els drons Bayraktar TB2,[93] especialitzats en la vigilància i el reconeixement.[94] Algunes webs apunten que, des del 2023, el Marroc ha adquirit drons armats Akinci,[95] que han estat registrats sobrevolant el territori de Smara, al Sàhara Occidental ocupat.[96] L'informe anual de l'organització Sahrawi Mine Action Coordination Office (SMACO), destaca 73 atacs amb drons marroquins contra civils, entre 2021 i 2023, que van causar 160 víctimes civils, entre les quals, 80 morts.[97] La naturalesa indiscriminada d'aquests atacs ha provocat greus ferides i morts entre la societat civil sahrauí, mauritana i algeriana, tota la població civil.[98] El desenvolupament de la tecnologia de drons i el final de l'alto el foc han anat acompanyats del desenvolupament de la Llei estructural marroquina núm. 10.20,[99] que a través dels seus 55 articles permet i fomenta la construcció d'unitats per a la indústria armamentística al Marroc, la fabricació d'armes, a través d'operadors nacionals i les inversions estrangeres en aquest sector.[100] Paral·lelament, la normalització de les relacions entre el Marroc i Israel, l'any 2020,[101] ha afavorit la cooperació militar entre els dos actors, fet que ah derivat en un memoràndum d'entesa entre tots dos països en matèria de defensa,[102]

---

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

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

95 **Bladi**, "Akinci Zoom: Le Drone que le Maroc Va Acquérir," Bladi.
Disponible a: 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 a:
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 maig del 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 a:
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 juliol del 2020.
Disponible a:
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 a: https://sedici.unlp.edu.ar/handle/10915/162819

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

l'any 2021. Després d'aquest acord, s'han conegut els plans de l'empresa israeliana Blue Bird Aero Systems per establir una planta de producció dels models de drons WanderB i ThunderB al Marroc, que es destinen principalment a missions de reconeixement, intel·ligència i detecció d'objectius.[103] Els atacs amb drons provoquen el desplaçament de la població sahrauí fora del seu territori alhora que es vulneren els seus drets, com el dret a l'habitatge, el dret al lliure moviment, la identitat cultural i el dret a la protecció contra el desplaçament arbitrari.

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

III

TUNISIA: L'ESTAT D'EMERGÈNCIA PERMANENT

Durant les dues dècades en què Tunísia va estar governada per l'autòcrata Zine el Abidine Ben Ali, derrocat el 2021, el Govern va estendre la vigilància als espais privats de la població, a través d'un aparell de seguretat especialment invasiu. Posteriorment a la caiguda del règim, després de la Revolució del gessamí del 2011, semblava que la situació es revertia i va créixer l'ús de la tecnologia per controlar el poder, per exemple, a través de la dinàmica de portar càmeres a les manifestacions i protestes per enregistrar els abusos policials. Va ser en aquell moment que va sortir a la llum el mecanisme de cibervigilància amb què l'Agencia Tunisiana d'Internet del Govern de Ben Ali havia estat censurant blogs i mitjans crítics amb el poder, que es coneixia amb el nom de Ammar 404[104] i que s'havia convertit en símbol de la vigilància durant la dictadura.[105]

Gairebé 15 anys després, Tunísia és avui un país en estat d'emergència permanent, que reaprofita parcialment l'arquitectura legal i tecnològica de la dictadura per seguir vigilant i reprimint jutgesses, periodistes, advocades, sindicalistes, oposició política i activisme LGBTIQ+, a través de lleis antiterroristes i contra la ciberdelinqüència.[106] Si bé és cert que Tunísia ha romàs a l'Índex de Llibertat de Premsa de Freedom House com el país àrab més garantista, la mateixa organització reconeix, al seu informe anual del 2023, que la població de Tunísia està perseguida per publicar a les xarxes contingut crític amb el president, el Govern o les forces de seguretat.[107]

1. RECUPERANT LES ESTRUCTURES DE VIGILÀNCIA DIGITAL DE LA DICTADURA

Durant els darrers anys del règim de Ben Ali, van conviure dues tendències paral·leles: l'augment de l'accés a internet de la població de Tunísia i el control ferri de les comunicacions, simbolitzat amb Ammar 404. Aquest era el missatge d'error que apareixia quan s'intentava accedir, des de l'interior del país, a una de les nombroses pàgines web censurades, entre les quals hi havia mitjans com Al Jazeera, Al Arabiya i mitjans digitals

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 a: https://journals.openedition.org/anneemaghreb/12646

105 **Webdo TN.** "Tunisie: Qui se cachait derrière Ammar 404 ?" 31 de gener del 2011.
Disponible a: https://www.webdo.tn/fr/actualite/national/qui-se-cachait-derriere-ammar-404/173718

106 **Amnistia Internacional.** "Túnez." Consultat el 25 d'octubre del 2024.
Disponible a: https://www.es.amnesty.org/en-que-estamos/paises/pais/show/tunez/

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

tunisians crítics com Nawaat.[108] [109] Aquest sistema s'encarregava de vigilar a blogueres i periodistes crítiques amb les autoritats. Els correus electrònics de la dissidència política eren interceptats de manera sistemàtica fent ús de tecnologies d'inspecció profunda de paquets (DPI),[110] [111] que el Govern tunisià hauria obtingut de les empreses estatunidenques Blue Coat System i Netapp, i de l'alemanya Ultimaco, segons van fer públic posteriorment algunes defensores de drets humans.[112] Per altra banda, Trovicor, antiga subsidiària de Siemens AG i Nokia Siemens, amb seu a Munic, haurien proporcionat al Govern tecnologies que permeten que es puguin fer servir per interceptar veu i dades i la millora de les eines per dur a terme escoltes.[113] Segons Privacy International, l'empresa danesa Sundby ETI A/S, subsidiària de BAE Systems hauria venut tecnologia d'intercepció de dades de telèfons mòbils capaç de "trackejar"[114] o rastrejar els hàbits de navegació de les usuàries i dur a terme registres de correus electrònics.[115]

Després de la caiguda de l'autòcrata el 2011, la Agència Tunisiana d'Internet (ATA), promotora del desenvolupament de la xarxa al país, va passar a estar sota la direcció de Moez Chakchouk, que va donar per desmantellat l'aparell de vigilància digital i el va substituir per una política d'obertura i democratització de l'accés a internet.[116] Tanmateix, la dinàmica de canvi no va durar gaire. L'any 2013, es va constituir l'Agència per a les Telecomunicacions (ATT), que opera sota el comandament del Ministeri de Comunicacions i Tecnologies de la informació i que "dona suport tècnic a les investigacions judicials sobre delictes relacionats amb la comunicació".[117] Activistes d'internet, com Afef Abrougui ja van advertir en aquell moment que s'estava recuperant el pretext de la lluita contra el terrorisme per

108 **Swissinfo.** "La primavera árabe: la primera revolución smartphone." 21 de gener del 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 setembre del 2008. Disponible a: https://advox.globalvoices.org/2008/09/24/tunisia-404-not-found

110 Vegeu glossari

111 **Privacy International.** "State surveillance in Tunisia." 2019. Disponible a: 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 juliol del 2014. Disponible a: 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 febrer del 2012. Disponible a: https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa

114 "Trackejar" és un terme que ve de l'anglès "to track" i fa referència a l'acte de seguir, monitorar o registrar la ubicació, el comportament, l'activitat d'alguna cosa o d'algú.

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

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

117 Decret 2013-4506 aprovat el 6 de novembre del 2013. Artículo 2.

"La manca de transparència en la compra pública de tecnologia no permet saber amb exactitud quines són les tecnologies de vigilància del règim de Ben Ali han seguit sent utilitzades pels Governs posteriors i se segueixen sent-ho actualment"

controlar la informació a la xarxa.[118] El retorn a les dinàmiques de vigilància i control del Govern anterior es reforçaria el 2015, arran d'una onada d'atemptats contra turistes perpetrats per l'autodenominat Estat Islàmic.[119] Poc després, es va aprovar la Llei 205/26 de lluita contra el terrorisme, durament criticada per organitzacions de drets humans locals i internacionals, que consideraven que el nou decret obria la porta novament al monitoreig i a la vigilància massiva.[120] Aquest any es va declarar també l'estat d'emergència, que ha seguit vigent durant l'última dècada. La manca de transparència en la compra pública de tecnologia no permet saber amb exactitud quines són les tecnologies de vigilància del règim de Ben Ali han seguit sent utilitzades pels Governs posteriors i se segueixen sent-ho actualment.[121]

2. VEDAT A LA LLIBERTAT D'EXPRESSIÓ AMB EL PRETEXT DE LA CIBERDELINQÜÈNCIA I LES *FAKE NEWS*[122]

Des de l'arribada al poder del president Kaïs Saïed, el 2019, s'ha intensificat de manera alarmant el setge contra defensores de drets humans i veus opositores al Govern. L'any 2020, Amnistia Internacional va publicar un informe amb els casos de 40 blogueres, administradores de pàgines populars de Facebook i defensores de drets humans, que havien estat condemnades per càrrecs com difamació, desacatament a les institucions estatals i "danys" a altri, a través de les xarxes socials. L'ONG expressava la seva preocupació

118 **Abrougui, Afef.** "Tunisians cast a wary eye on new crime agency - Index on Censorship". Index on Censorship, 2 de gener del 2014.
Disponible a: 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 febrer del 2019.
Disponible a: https://www.bbc.com/news/world-africa-47183027

120 **Human Rights Watch.** "Tunisia: Counterterror Law Endangers Rights". 31 de juliol del 2015.
Disponible a: 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 a: https://ccprcentre.org/files/documents/INT_CCPR_ICS_TUN_30055_E.pdf

122 Vegeu glossari

per la tendència creixent a comprometre la llibertat d'expressió a les xarxes amb l'ús de l'arquitectura legal i punitiva del règim.[123] Aquest és el cas de la bloguera tunisiana Emna Chargui, que va publicar a Facebook un text satíric sobre la COVID-19 i les mesures de confinament, en forma de versicle de l'Alcorà. A més de rebre amenaces de mort i de violència sexual (una forma d'atac utilitzada freqüentment contra les dones i les persones LGBTIQ+) per part de persones no identificades, Chargui va ser condemnada a sis mesos de presó per "ofendre els sentiments religiosos", mentre que les amenaces que va rebre encara no han estat investigades.[124]

Aquesta tendència es va accelerar de manera dramàtica el 2021, quan 60 organitzacions de drets humans van denunciar l'onada de repressió contra defensores de drets humans tunisianes. La repressió també incloïa l'assassinat de dues persones i vora 2000 detencions en només 2 mesos, nombrosos casos d'assetjament policial, a través de les xarxes socials, la condemna a 6 mesos de presó de l'activista queer Rania Amdouni o les tortures a joves, a comissaria.[125] El president Saïed va aprofitar el malestar al carrer, degut, en part, a les mesures restrictives decretades durant la pandèmia de la COVID-19, per congelar l'activitat al Parlament i va dissoldre el Govern, alhora que s'atorgava plens poders constitucionals, sota el pretext que Tunísia estava al caire d'un "perill imminent".[126]

L'any 2022, es va aprovar una nova constitució que preveia la possibilitat de suspendre el dret a la privacitat, recollit a la Carta Magna del 2014, en el cas que el país es trobés en "estat d'emergència".[127] Un estat d'emergència que estava vigent quan es va adoptar el nou text i que s'ha prolongat per decret fins al desembre del 2024.[128] Poc després, es va aprovar el decret llei núm. 2022-54 del 13 de setembre del 2022, la coneguda com a "Llei de Ciberde-

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

124 **Amnistia Internacional.** "Tunisia: Blogger Emna Chargui sentenced to six months in prison for social media post." 9 de novembre del 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 març del 2021."
Disponible a:
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 juliol del 2021.
Disponible a:
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 a: 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 gener del 2024.
Disponible a:
https://www.europapress.es/internacional/noticia-presidente-tunez-anuncia-ampliacion-otro-ano-mas-largo-estado-emergencia-20240131024235.html

linqüència", que castiga la difusió d'informació falsa de manera malintencionada, a través de xarxes digitals. Aquesta llei fa servir termes ambigus com ara *fake news*[129] i atorga a les autoritats el poder de tancar mitjans de comunicació i organitzacions de la societat civil, en cas que se'n violi l'articulat.[130] La llei estableix disposicions per permetre a les autoritats "recollir proves electròniques" recopilar dades personals i interceptar comunicacions privades, a partir de criteris vagues. Des d'aleshores, més de 40 persones han estat detingudes de manera arbitrària per la seva defensa de drets o llibertat d'expressió bona part d'elles per "conspiració", sota la Llei de la Ciberdelinqüència. La majoria d'aquestes persones fa mesos que es troben en presó preventiva a l'espera de judici, en alguns casos, fa més d'un any.[131]

"la lluita contra la ciberdelinqüència es focalitza especialment en persones joves que a Tunísia han estat catalitzadores de mobilitzacions importants després de les Primaveres Àrabs, per la manca de perspectives de feina i futur"

Aquesta repressió en nom de la lluita contra la ciberdelinqüència es focalitza especialment en persones joves que a Tunísia han estat catalitzadores de mobilitzacions importants després de les Primaveres Àrabs, per la manca de perspectives de feina i futur. Un dels casos més coneguts és el de l'estudiant Ahmed Hamada, que administrava una pàgina de Facebook on es publicaven els abusos policials contra el veïnat de classe treballadora del barri de Hay Tadhamin, a la capital. Hamada va ser detingut l'octubre del 2022 i el seu ordinador i el seu telèfon varen ser requisats per extreure'n les dades. S'enfronta a 12 anys de presó per "utilitzar sistemes de comunicació per expandir intencionadament *fake news* contra agents de l'Estat".[132]

129 Vegeu glossari

130 **Amnistia Internacional.** "La Tunisie doit abroger le décret relatif à la cybercriminalité". 12 de desembre del 2022. Disponible a: 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 desembre del 2023.
Disponible a:
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." Juliol del 2023.
Disponible a:
https://www.icj.org/wp-content/uploads/2023/07/Tunisia-Silencing-Free-Voices-_compressed-1.pdf

3. INTERCEPCIÓ DE LES COMUNICACIONS I PIRATEIG DE DISPOSITIUS

A banda de la Llei de Ciberdelinqüència, la renovació de l'estat d'emergència el 2023 va garantir a l'Agència Tunisiana de Telecomunicacions (ATI) l'accés als continguts de dispositius electrònics sense ordre judicial i li va conferir plens poders per confiscar dispositius, extraure dades i interceptar comunicacions.[133]

El febrer del 2024, es van encausar 17 persones de partits de l'oposició, funcionaris de l'Estat i membres de la iniciativa "Citizens agains the coup", que exigeix la fi de l'estat d'emergència, sota la llei antiterrorista del 2015, acusades de conspirar per derrocar el president Saïed. A algunes de les persones acusades se'ls van confiscar els telèfons mòbils i inclús les targetes d'emmagatzematge, segons una investigació del mitjà crític Inkyfada, que va tenir accés a l'expedient judicial. Durant els interrogatoris, també es van fer servir extractes de converses de WhatsApp, Telegram i inclús Signal,[134] que suposadament havien mantingut amb diplomàtics estrangers.

Tal com passa a la resta de la regió, les persones LGBTIQ+ són un dels objectius principals a Tunísia, on les pràctiques sexuals entre persones del mateix sexe estan penades amb fins a 3 anys de presó.[135] La digitalització de les relacions al país ha comportat la criminalització de l'anomenada "immoralitat digital" que s'ha materialitzat en la hipervigilància i l'exposició de dades i d'informació íntima de desenes de persones LGBTIQ+.[136] Una de les tendències creixents en aquest sentit és l'extracció d'informació de dispositius, sigui mitjançant accés no consentit, pirateig o amenaces. Human Rights Watch relata el cas d'una parella d'homes que van ser interrogats sobre el seu activisme LGBTIQ+ per agents de policia, que els van exigir veure les seves converses i pàgines de Facebook. Malgrat que s'hi van negar, els agents els van confessar que, en realitat, ja havien accedit a la informació, gràcies al propietari de casa seva que els havia donat consentiment perquè accedissin al wifi i pirategessin els seus comptes de correu, els

133 **Freedom House**. 2023. Disponible a: 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 març del 2023.
Disponible a: 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 febrer del 2021.
Disponible a:
https://www.hrw.org/fr/news/2021/02/23/tunisie-arrestations-arbitraires-dactivistes-lgbti-et-violences-policieres

seus telèfons i els seus ordinadors portàtils[137] i recopilessin una bona quantitat d'informació privada.

A més, les activistes LGBTIQ+ s'enfronten als atacs perpetrats per trols o exèrcits electrònics,[138] organitzats a les xarxes socials, on se'ls denigra i s'incita a la violència en contra seva. L'any 2021, un grup de defensores de drets humans que enarboraven la bandera de l'arc de Sant Martí en una manifestació a Tunísia capital va ser sotmès a assetjament en línia, en alguns casos per part de pàgines de Facebook associades a sindicats policials. És el cas de l'artista lesbiana Rania Amdouni, de qui circulen centenars de fotografies amb amenaces de mort, el telèfon i l'adreça de la qual van ser filtrats per trols.[139] [140] En alguns casos, aquestes persones arriben a fugir del país per la inseguretat que senten (sexili).

4. INVERSIÓ OCCIDENTAL MILIONÀRIA PER A LA VIGILÀNCIA DE FRONTERES

Bona part de la tecnologia més sofisticada que es fa servir el Govern es vehicula cap a la vigilància de la costa tunisiana i de la frontera amb Líbia, amb l'objectiu de controlar no només la migració a Europa, sinó també la presència de grups islamistes violents, especialment després dels atemptats del 2015. Del 2016 al 2018, el Govern va construir un mur de 200 kilòmetres al llarg de la seva frontera amb Líbia, equipat amb sistemes d'alta resolució i abast de llarga distància, càmeres tèrmiques i amb detecció de moviments, vinculades a una central de vigilància. El projecte va ser finançat per Alemanya[141] i els Estats Units[142] d'Amèrica i el va executar la URS, filiar de la multi-

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 Vegeu glossari

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

140 Vegeu glossari

141 **Webdo.** "Des équipements de surveillance électronique allemands à la Tunisie." 16 d'octubre del 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 d'agost del 2016.
Disponible a:
https://kapitalis.com/tunisie/2016/08/14/des-americains-installent-la-surveillance-electronique-au-sud-de-la-tunisie

"La dinàmica de coartar la llibertat de moviments i de sortida del país a les persones que migren des de Tunísia s'ha agreujat els últims anys, juntament amb les campanyes racistes i d'assetjament i difamació a les xarxes"

nacional d'enginyeria AECOMS, totes dues estatunidenques.[143] [144]

Recentment, el Govern ha adquirit un sofisticat sistema de reconeixement digital i identificació biomètrica proporcionat pel gegant francès Idemia.[145] La justificació per posar en marxa aquests sistemes és reforçar les capacitats tècniques i operacionals en seguretat de fronteres i la persecució de grups "terroristes". La dinàmica de coartar la llibertat de moviments i de sortida del país a les persones que migren des de Tunísia s'ha agreujat els últims anys, juntament amb les campanyes racistes i d'assetjament i difamació a les xarxes alimentades pel mateix president Saïed.[146] També s'ha denunciat violència, incloent-hi violència sexual, contra les dones migrants, com publica recentment The Guardian.[147] Des del 2013, el Ministeri de l'Interior de Tunísia ha imposat restriccions de circulació a gairebé 30 000 persones, en virtut de les mesures de control de les fronteres, que no són públicament accessibles i no compten amb cap mena de supervisió judicial, tal com denunciava Amnistia Internacional en un informe publicat el 2018.[148]

---

143 Ibid.

144 **Webdo.** "Le système de surveillance électronique à la frontière tuniso-libyenne". Disponible a: 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 març del 2024. Disponible a: https://www.actu-maroc.com/kais-saied-lance-un-programme-de-securite-numerique-en-tunisie-malgre-la-crise-economique/

146 **Amnistia 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 setembre del 2024. Disponible a: 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 d'octubre del 2018. Disponible a: https://www.amnesty.org/es/latest/press-release/2018/10/tunisia-arbitrary-and-abusive-travel-restrictions-breach-human-rights/

IV

EGIPTE: L'ESTAT COM A HACKER MALICIÓS I ASSETJADOR EN LÍNIA

Quan la Primavera Àrab va arribar a la plaça Tahrir de El Caire, el 2011, el Govern de Mubarak va ampliar la tecnologia disponible per interceptar trucades de telèfon i estrènyer el setge contra les defensores de drets humans que lluitaven contra el règim. L'any 2016, un informe de Privacy International posava de manifest l'existència d'una unitat secreta, el Departament d'Investigació Tècnica (TRD, per les seves sigles en anglès) atribuïda al Servei General d'Intel·ligència egipci, que hauria adquirit tecnologia de vigilància de la finlandesa Nokia Siemens Network.[149] Després del cop militar del president del Consell Suprem de les Forces Armades, Abdul Fatah al-Sisi, contra l'aleshores president electe sorgit després de les revoltes: Mohamed Morsi l'any 2013, la situació no només no va millorar pel que fa a la llibertat d'expressió i als drets polítics; sinó que la llibertat a internet i els drets dels usuaris es van restringir severament, tal com assenyala l'informe de *Freedom on the Net* del 2023.[150] Les sancions penals, l'assetjament i la vigilància han contribuït a convertir el periodisme crític amb el Govern en una activitat impossible i han impulsat la censura i l'autocensura.

Al seu torn, les agències de seguretat han adquirit a empreses occidentals tecnologia sofisticada per l'espionatge, el control i la intercepció de les comunicacions, dinàmica que han dut a terme de manera extremadament exhaustiva, mentre desenvolupaven una indústria pròpia de la vigilància.[151] La censura massiva de pàgines web, que es calcula en més de 600 webs bloquejades, des del 2017 i la persecució i l'assetjament a periodistes, defensores de drets humans i persones LGBTIQ+, han convertit el país nord-africà en un client prolífic i un autèntic laboratori per a les tecnologies de vigilància massiva i monitoreig en línia d'empreses occidentals.

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

150 **Freedom House.** "Freedom on the Net 2023, Country: Egypt."
Disponible a: 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 gener del 2020.
Disponible a:
https://timep.org/2020/01/31/global-tech-and-domestic-tactics-egypts-multifaceted-regime-of-information-controls/

1. ROBATORI DE CREDENCIALS I ACCÉS FRAUDULENT ALS COMPTES DE CORREU D'ONG DE DRETS HUMANS.

A Egipte, el Govern d'Al-Sisi és extremadament actiu pel que fa a l'assetjament digital a la societat civil, si es té en compte la gran quantitat d'informes i denúncies de defensores de drets humans que s'han fet públiques en els darrers anys. La seva acció no es limita a la clàssica intercepció de les comunicacions per aplicacions de missatgeria o telefòniques, sinó que utilitza tots els mitjans al seu abast. El 2017, va sortir a la llum una campanya de *phishing*[152] anomenada "Nile Phish" (peix del Nil) contra un mínim de set ONG de drets humans i defensores de drets humans, advocats i periodistes de país.[153] Segons una investigació de l'organització Citizen Lab, l'ús d'aquesta tècnica informàtica va resultar en el pirateig de desenes de comptes de Gmail i Dropbox. En aquest cas, les víctimes es van infectar a través d'un fals correu de l'organització Nadeem Center for Rehabilitation of Violence (clausurada per les autoritats egípcies, des d'aleshores) i intentava obrir un enllaç per obtenir més informació sobre una suposada conferència. L'atac va ser orquestrat amb l'ús d'una plataforma de font oberta i gratuïta anomenada GoPhish, que permet crear simulacions realistes d'usuaris fiables.[154]

"el Govern d'Al-Sisi és extremadament actiu pel que fa a l'assetjament digital a la societat civil"

El març del 2019, una investigació d'Amnistia Internacional va posar de manifest una altra onada d'atacs digitals que "probablement els van originar organismes que tenen el suport del Govern"[155] i que va implicar nombrosos intents d'obtenir accés als comptes de correu electrònic de diverses defensores de drets humans, mitjans de comunicació i personal d'organitzacions egípcies. [parcial]Aquesta nova campanya es produïa enmig d'allò que l'ONG considerava una ofensiva sense precedents, que ha convertit Egipte en una presó

152 Vegeu glossari

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 a: https://citizenlab.ca/2017/02/nilephish-report/?ref=hackernoon.com

155 **Amnistia Internacional.** "Phishing attacks using third-party applications against Egyptian civil society organizations". 6 de març del 2016. Disponible a: https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

"a l'aire lliure per a les veus crítiques".[156] En aquest cas, els atacants no varen recórrer a mètodes tradicionals de pesca o *phishing*[157] per robar credencials, sinó que van utilitzar una manera més sigil·losa i eficient d'accedir a les safates d'entrada de les víctimes. Es tracta d'una tècnica coneguda com *OAuth Phishing*[158] que enganya les usuàries per a que atorguin permisos a aplicacions malicioses que poden accedir a les dades del seu compte i dur a terme accions en nom seu. Bàsicament, els atacants varen enganyar les víctimes perquè els concedissin accés total als seus correus electrònics, a través d'aplicacions mòbils allotjades a la Play Store oficial del Google i Android.[159]

"Els atacants varen enganyar les víctimes perquè els concedissin accés total als seus correus electrònics, a través d'aplicacions mòbils allotjades a la Play Store oficial del Google i Android"

Segons un informe publicat mesos després per Check Point Research, la plataforma d'intel·ligència de l'empresa israeliana CheckPoint Software Technologies, l'atac va afectar a 33 periodistes, polítiques, advocades i defensores de drets humans, els correus electrònics, els contactes i la ubicació dels quals van ser interceptats i enregistrats.[160] CheckPoint no va trobar cap relació directa i irrefutable amb els serveis d'intel·ligència egipcis, tot i que la plataforma va considerar que donats "els objectius, la clara intenció i propòsit de les aplicacions, l'estructura i les dades descarregades, així com un servidor registrat al Ministeri de Tecnologies de la Informació i una ubicació codificada que correspon a la seu de la principal agència d'espionatge d'Egipte, és gairebé segur que es va tractar d'una acció impulsada pel Govern".[161]

156 Ibid.

157 Vegeu glossari

158 Vegeu glossari

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

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

161 Ibid

2. ESPIONATGE I MINERIA DE DADES AMB TECNOLOGIA I CAPITAL ISRAELIANS

Entre maig i setembre del 2023, l'ex parlamentari egipci Ahmed Eltantawy va ser objecte de diversos intents d'infectar el seu telèfon mòbil amb el programari espia[162] Predator de Cytrox després d'anunciar la seva intenció de presentar-se a les eleccions presidencials del 2024.[163] Aquest tipus de programa permet monitorar dispositius infectats, independentment de la seva ubicació, en temps real.[164] Cytrox forma part d'Intellexa Consortium, un grup d'empreses de programari espia[165] i serveis relacionats conegudes per competir amb NSO Group i vendre tecnologia als països als quals NSO ja no ven els seus productes, després d'escàndols relacionats amb el seu impacte en les violacions dels drets humans.[166] El març de 2024, el Departament del Tresor dels Estats Units va sancionar Cytrox i Intellexa Consortium per vendre eines d'espionatge i vigilància massiva a règims autoritaris i "pel seu paper en el desenvolupament i distribució de programari espia[167] utilitzat contra ciutadans nord-americans, inclosos membres del Govern, periodistes i assessors".[168]

La connexió mòbil d'Eltantawy va ser atacada persistentment mitjançant injecció de xarxa.[169] Quan visitava determinats llocs web que no utilitzaven HTTPS, un dispositiu instal·lat a la frontera de la xarxa de Vodafone Egipte el redirigia automàticament a un lloc web maliciós, per infectar el seu telèfon amb el programa espia, alhora que rebia enllaços per SMS i WhatsApp per facilitar que caigués a la trampa. L'ex parlamentari, que sospitava que podia ser víctima d'un intent d'infecció, es va posar en contacte amb la plataforma

162 Vegeu glossari

163 **Attalah, Lina.** "Aspiring presidential candidate Ahmed Tantawi targeted by Predator spyware", Mada. 14 de setembre del 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 a: https://www.sekoia.io/en/glossary/predator-spyware/

165 Vegeu glossari

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 a:
https://r3d.mx/2024/03/20/estados-unidos-sanciona-al-ceo-de-intellexa-empresa-creadora-de-spyware-por-violaciones-a-derechos-humanos/

167 Vegeu glossari

168 **Departament del Tresor dels EUA.** "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium". 05 de març del 2024.
Disponible a: https://home.treasury.gov/news/press-releases/jy2155

169 Vegeu glossari

Citizen Lab.[170] En el comunicat on confirmava les sospites de Eltantawy, Citizen Lab assegurava que "atès que Egipte és un client conegut del programa espia Predator de Cytrox, i que aquest es va lliurar a través d'injecció de xarxa,[171] des d'un dispositiu situat físicament dins d'Egipte, atribuïm l'atac d'injecció de xarxa al Govern egipci, amb alta probabilitat".[172] Durant el mateix període, les forces de seguretat van detenir diversos voluntaris de la seva campanya política.[173]

3. TECNOLOGIA CANADENCA PER A LA CENSURA DE PÀGINES WEB CRÍTIQUES

La censura de pàgines web a gran escala, a més d'una tendència regional, és també una dinàmica destacada en el context egipci. Des del 2017, hi ha més de 600 webs i dominis que són inaccessibles de l'interior del país. El 2020, diverses organitzacions egípcies, regionals i internacionals, com ara Cairo Institute for Human Right Studies (CIHRS) o la Electronic Frontier Foundation (EFF) van denunciar aquest fenomen i van assenyalar que aquesta dinàmica constituiria una violació del dret a l'accés a la informació i

"La censura de pàgines web a gran escala, a més d'una tendència regional, és també una dinàmica destacada en el context egipci. Des del 2017, hi ha més de 600 webs i dominis que són inaccessibles de l'interior del país"

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

171 Vegeu glossari

172 **Scott-Railton, John et al.** "Predator in the wires. Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions". Citizenlab. 22 de setembre del 2023.
Disponible a:
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 maig del 2023.
Disponible a:
https://www.madamasr.com/en/2023/05/28/news/u/presidential-hopeful-ahmed-tantawi-friends-disappeared-before-reaching-campaign-hq/

a la llibertat d'expressió.[174] Les webs pertanyen a mitjans de comunicació crítics, plataformes polítiques i de denuncia de vulneracions de drets humans, com el mitjà de periodisme social Al-Manassa, que ha estat objecte de persecució i bloqueig des de poc després de la seva creació, el 2016.[175] Les autoritats egípcies fins i tot han bloquejat els dominis alternatius als quals va recórrer el lloc per continuar operant. Al juny de 2020, les forces de seguretat van escorcollar les oficines d'Al-Manassa[176] i van arrestar l'editora en cap, Nora Younis, que va ser detinguda durant tres dies acusada d'operar un lloc sense llicència i de cometre delictes cibernètics abans de ser alliberada sota fiança. Younis es va convertir en la primera periodista egípcia a enfrontar-se a acusacions sota la llei de delictes cibernètics, tot i que Al-Manassa havia presentat una sol·licitud de llicència i havia pagat les taxes corresponents el 2018.[177] [178] [179]

La restricció d'accés a determinats continguts i el tancament de webs es va dur a terme apellant a la Llei de regulació de mitjans de premsa i la Llei de delictes cibernètics, aprovada el 2018, que amplia els poders per a la vigilància en línia, el bloqueig de webs, la intercepció de comunicacions i el monitoreig d'internet.[180] L'article 7 de la Llei de delictes cibernètics atorga a l'autoritat investigadora el poder de tancar un lloc web, sempre que es consideri que el contingut constitueix un delicte o una amenaça per la seguretat nacional o l'economia.

---

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 novembre del 2021.
Disponible a:
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 a:
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. Desembre de 2021.
Disponible a:
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 d'octubre del 2020.
Disponible a: 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 juny de 2020.
Disponible a: 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 juny de 2020.
Disponible a: 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 juny del 2018.
Disponible a:
https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians

Al-Manassa va sol·licitar els serveis d'anàlisi forense digital de l'ONG sueca Qurium[181], dedicada a la defensa dels drets digitals, protecció de dades i la seguretat a Internet. La investigació va revelar que els proveïdors d'internet egipcis fan servir una tecnologia anomenada inspecció profunda de paquets (DPI, per les seves sigles en anglès)[182] per restringir l'accés a determinats continguts i pàgines web. Segons el mitjà digital tecnològic estatunidenc The Verge, la inspecció profunda de paquets és una de les tecnologies més invasives que un país pot utilitzar en la seva xarxa d'Internet. "Aquesta tècnica emprada per règims autoritaris, des de Rússia fins a Bahrain, permet als Governs examinar el contingut del trànsit web, a mesura que es navega per la xarxa, cosa que els permet censurar llocs web a temps real i dur a terme una vigilància detallada de les activitats de la societat civil, a la xarxa. També requereix un equip sofisticat, que normalment proporciona una empresa occidental",[183] assegura el mitjà digital.

En aquest cas, va ser Sandivine,[184] una empresa canadenca que, des del 2017 i fins a l'agost del 2024, era propietària del grup inversor Francisco Partners, també accionista de NSO Group, fins el 2019. El febrer del 2024, es va fer públic que el Departament del Tresor dels Estats Units d'Amèrica havia inclòs Sandivine en una llista per la implicació de la seva tecnologia DPI[185] a la censura en línia i l'espionatge de defensores de drets humans a Egipte.[186] Després de l'escàndol, Francisco Partners va decidir prescindir de Sandivine i actualment està en venda per 450 milions de dòlars.[187]

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

182 Vegeu glossari

183 **Brandom, Russell.** "Egypt Launches Deep-Packet Inspection System". The Verge. 17 de setembre del 2014.
Disponible a:
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 febrer del 2024.
Disponible a: https://www.theregister.com/2024/02/27/sandvine_us_entity_list

185 Vegeu glossari

186 D**epartament d'Estat dels EUA.** "The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses." el 28 de febrer del 2024.
Disponible a:
https://www.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-abuses/

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

4. CAMPANYES COORDINADES D'ASSETJAMENT I EMBOSCADES DIGITALS CONTRA DEFENSORES DE DRETS HUMANS[188]

Un altre dels mecanismes de vigilància utilitzat habitualment contra defensores de drets humans és l'assetjament a les xarxes socials, sovint alimentat amb bots. Aquest assetjament sol intensificar-se en moments puntuals, on l'atenció mediàtica està centrada a Egipte i el règim no es pot permetre que la situació d'autoritarisme asfixiant es difongui més enllà de les seves fronteres.

El desembre de 2020, un hashtag denigrant contra el director de l'organització Egyptian Initiative for Personal Rights (EIPR), Hossam Bahgat, es va fer viral el país i va omplir la xarxa X (abans Twitter) de contingut homòfob i deshumanitzador. L'atac, seguit per centenars de trols[189] i bots, alguns d'ells pro Govern,[190] formava part d'una ofensiva més àmplia contra el personal d'aquesta organització de defensa dels drets humans egípcia. Tres dels membres d'aquesta ONG van ser detinguts en el mateix període, després d'una visita de 13 diplomàtics a la Seu de l'organització, i van ser alliberats dies més tard.[191]

"Un hashtag denigrant contra el director de l'organització Egyptian Initiative for Personal Rights (EIPR), Hossam Bahgat, es va fer viral el país i va omplir la xarxa X (abans Twitter) de contingut homòfob i deshumanitzador. L'atac, seguit per centenars de trols i bots, alguns d'ells pro Govern"

No va ser l'únic mètode d'assetjament contra Bahgat. El gener del 2019, després de fer una piulada crítica a X, centenars de comptes falsos van començar a seguir el seu compte a X cada minut, durant un parell de dies. Lluny de ser innòcua, aquesta tècnica d'atac generalment condueix al tancament o suspensió del compte perquè s'associa amb el comportament dels bots.

188 Vegeu glossari

189 Vegeu glossari

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

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

Durant les setmanes prèvies a la cimera sobre el clima COP27, el 2022, més de 150 persones van ser detingudes i investigades per la Fiscalia Superior de Seguretat de l'Estat egipci, per haver fet servir les xarxes socials per convocar les protestes contra la cimera.[192] A més, es va fer públic que l'aplicació mòbil de la COP27, desenvolupada pel Ministeri de Comunicacions i Tecnologies de la Informació egipci, permetia a les autoritats escoltar converses, accedir a correus privats i rastrejar missatges, incloent-hi els xifrats.[193] Aplicació va ser titllada de "ciberarma" tot i que no es va poder demostrar que aquesta vigilància s'estigués produint.

Com passa a la resta de la regió, però en el cas d'Egipte, de manera especialment violenta, les persones LGBTIQ+ segueixen sent un objectiu prioritari de l'assetjament i la repressió en línia. Des de finals del 2013 i fins al 2017, la mitjana anual de detencions va ser de 66, mentre que el 2019 van ser 92 les persones detingudes, sospitoses d'haver mantingut pràctiques homosexuals.[194] L'ús d'aplicacions de cites com Grind, Hornet i Growler, habituals en el col·lectiu LGBTIQ+ s'ha convertit en una font de risc, que s'afegeix a l'extrem nivell de vigilància en línia fora de línia. És el cas d'un home gai, que va ser detingut durant 11 dies l'any 2018, després que li tendissin una trampa, en la qual un oficial de policia s'hi va posar en contacte i li va fer creure que tenia un interès romàntic, per tot seguit aturar-lo en un *checkpoint* i obligar-lo a mostrar el contingut del seu telèfon mòbil.[195] A més a més, després de l'aprovació de la Llei contra els ciberdelictes, l'any 2018, els casos contra les persones LGBTIQ+ es jutgen no només com un greuge a la moralitat, sinó com un ciberdelicte, fet que permet a les autoritats imposar sentències més dures i condemnes més estrictes.[196]

Les Primaveres Àrabs del 2011 al Líban varen sembrar la llavor de la indignació que va germinar en nous alçaments populars més sòlids i massius en anys posteriors. Les mobilitzacions populars del 2011 exigien la fi del sistema confessional i sectari al país. La mobilització només va durar tres mesos,[197] però així i tot, la indignació va seguir latent i gradualment van

192 **Coogle, Adam.** "Egypt: Arrests, Curbs on Protests as COP27 Nears". Human Rights Watch. 6 de novembre del 2022. Disponible a: 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. 9 de novembre del 2022.
Disponible a: 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 desembre del 2020.
Disponible a: 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 d'abril del 2018.
Disponible a: 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 desembre del 2020.
Disponible a: https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html

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 febrer del 2023
Disponible a:
https://www.arab-reform.net/publication/from-overthrowing-the-regime-to-all-means-all-an-analysis-of-the-lebanonisation-of-arab-spring-rhetoric/

emergir noves campanyes com l'any 2013 (#NoToExtention) i el 2015 ("*YouStink*"). Va ser en aquest marc, on es va començar a fer servir l'eslògan "*All Means All*", que va donar visibilitat i sentit a les protestes del 2019 contra el Govern i el sistema bancari, on van participar de forma activa dones migrants i treballadores domèstiques,[198] moltes de les quals treballen al país en un règim de semi esclavatge.[199] Aquest procés va representar l'emergència d'una nova generació de defensores de drets humans, que va combinar de manera hàbil les noves tecnologies digitals per a l'organització i la mobilització social.

Davant d'aquest auge popular, el Govern va reaccionar reforçant els sistemes de vigilància massiva. El 2018 va sortir a la llum pública una sofisticada infraestructura de ciberespionatge, coneguda com a Dark Caracal, vinculada a la Direcció General de Seguretat General libanesa (GDGS per les seves sigles en anglès), que des del 2012 havia llançat múltiples campanyes de vigilància massiva, amb tecnologies avançades d'empreses occidentals.[200] Els drets civils i digitals de la població libanesa també estan essent amenaçats, en part, per un marc regulador restrictiu i dèbil en termes de protecció de drets a la privacitat, però també per les vulnerabilitats de la infraestructura digital del país, tal com es va demostrar durant el ciberatac contra la plataforma de registre de passatgers (MOPHPASS), creada pel Ministeri de Sanitat per a la gestió de la COVID-19.[201] Més recentment, l'atac massiu contra dispositius cercapersones i walkie-talkies de militants de Hezbollah ha demostrat també la capacitat tecnològica d'Israel per atacar en territori libanès.[202]

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

199 **Kvinna till Kvinna.** "Abolishing modern slavery in Lebanon." 27 de març del 2023.
Disponible a: 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 gener del 2018.
Disponible a: 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 juny del 2022.
Disponible a:
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 setembre del 2024.
Disponible a: https://www.eldiarioar.com/mundo/israel-coloco-explosivos-miles-buscas-importados-hizbula-acelero-ataque-temor-descubierto_1_11663562.html

V

EL LÍBAN: CIBERESPIONATGE, CENSURA I VIOLÈNCIA DIGITAL AL LÍBAN

1. CIBERESPIONATGE MASSIU A LA POBLACIÓ

Els darrers 20 anys, l'ús d'internet a la societat libanesa ha passat del 9 % al 90 %.[203] A finals del 2021, prop de 4,2 milions de libaneses, aproximadament el 76 % de la població total, tenien una subscripció de telefonia mòbil.[204] En aquest context, les principals agències d'intel·ligència del Líban, com el GDGS, les Forces de Seguretat Internes (ISF) del Ministeri de l'Interior i la Direcció General d'Intel·ligència Militar (MID) del Ministeri de Defensa disposen cadascuna dels seus propis sistemes de vigilància, sobretot tecnologies per interceptar comunicacions.[205] El MID també disposa de sistemes de monitoreig i extracció de dades de les xarxes socials. A més, el MID rep suport del Regne Unit en el marc de l'estratègia "Prevent" per lluitar contra l'extremisme violent.[206]

La intercepció de comunicacions és una pràctica habitual de les agències d'intel·ligència libaneses. En teoria, la Llei 140/1999 sobre Intercepció de Comunicacions estableix que les comunicacions personals (telèfon, fax, correus electrònics) estan protegides sota la llei i que només es poden interceptar en casos d'extrema urgència i sota ordre judicial o administrativa.[207] Tanmateix, en la pràctica, aquestes garanties judicials no es donen. Segons Privacy International, no hi ha garanties que els serveis d'intel·ligència estatals interceptin comunicacions de manera massiva, sense cap supervisió legal.[208] Des de l'assassinat del primer ministre Rafiq Hariri, el 2005, en diverses ocasions, les ISF han tingut accés il·limitat a dades de telecomunicacions de la societat libanesa, sempre amb l'autorització del Consell de Ministres.[209]

Paral·lelament, des de les Primaveres Àrabs, els serveis d'intel·ligència libanesos han anat adquirint tecnologies i serveis d'empreses occidentals per a la vigilància massiva de la societat civil. El 2015, l'MID va adquirir, per 1,4 milions de dòlars, el software de vigilància massiva "*Remote Control System*" de l'empresa italiana Hacking Team, que permetia enregistrar vídeos i fer

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

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

205 Analista digital, entrevista realitzada per l'equip d'investigació, 9 de setembre del 2024.

206 **Government of the United Kingdom.** "MENA Lebanon Security Programme Summary FY 18/19."
Disponible a:
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 gener del 2019.
Disponible a: https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

208 Ibid.

209 Ibid.

captures de pantalla i monitorar la localització GPS dels mòbils.[210] Així mateix, el centre d'investigació de la Universitat de Toronto, Citizen Lab, va informar sobre l'ús del programari espia[211] de l'empresa britànica Gamma Group, dissenyat per infectar ordinadors i obtenir la informació que contenen. Segons aquest centre, les agències d'intel·ligència de l'ISF i el GDGS van fer servir aquesta tecnologia el 2015.[212]

"la pobre alfabetització mediàtica al Líban, exposa a la societat civil al *phishing* i als programaris espia als seus ordinadors i dispositius mòbils"

No obstant això, el principal sistema utilitzat per a la vigilància massiva al Líban va ser la infraestructura Dark Caracal. El 2018, les organitzacions Lockout i Electronic Frontier Foundation (EFF) van publicar l'informe "Dark Carcal". Ciberespionatge a gran escala" on es descriu un sistema de ciberespionatge massiu amb capacitat per poder emprar Amenaces Persistents Avançades (APT, per les seves sigles en anglès)[213] administrat des del GDGS a Beirut, des del 2012.[214] Més concretament, Dark Carcal va dur a terme "campanyes de vigilància" de manera periòdica, tot combinant sistemes de pirateig tradicionals, amb sistemes avançats de vigilància massiva com l'anomenat Pallas o el programari espia[215] de FinFisher, capaços d'extraure informació d'SMS, aplicacions de missatgeria, captures de pantalla, enregistraments d'àudio, localitzacions de punts d'accés wifi i SSIDs.[216] Segons EFF i Lockout, aquest sistema va obtenir centenars de gigabytes d'informació d'institucions financeres, empreses, contractistes de seguretat i defensa, militars, institucions educatives, periodistes, advocades i defensores de drets humans en més de 21 països.[217] En aquest sentit, Ralph Baydoun, analista digital libanès, afegeix que la pobre alfabetització mediàtica al Líban, exposa a la societat civil al *phishing*[218] i als programaris espia[219] als seus ordinadors i dispositius mòbils.[220]

---

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

211 Vegeu glossari

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

213 Vegeu glossari

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

215 Vegeu glossari

216 Les sigles SSID venen del terme Service Set Identifier i volen dir identificador del conjunt de serveis. Es tracta del nom que té una xarxa wifi per poder trobar-la i identificar-la entre altres xarxes i connexions.

217 Ibid.

218 Vegeu glossari

219 Vegeu glossari

220 Ralph Baydoun, entrevista personal realitzada per l'equip d'investigació, 6 de setembre del 2024.

Així i tot, malgrat tots aquests sistemes avançats d'espionatge, l'arquitectura de ciberseguretat al país és molt dèbil. Al Líban, hi ha webs governamentals i infraestructures crítiques que són piratejades de manera sistemàtica. Alguns exemples recents van ser el pirateig dels panells informatius de l'aeroport internacional de Beirut[221] o les pàgines del Ministeri d'Afers Socials i del Parlament Libanès, a mans d'un grup de pirates informàtics contractat presumiblement per actors israelians.[222] Segons l'Imad Bazzi, periodista d'investigació libanès, aquesta situació evidencia el caos de la ciberseguretat al seu país, però també indica que el Govern no té capacitats tan sofisticades com per monitorar de manera exhaustiva la població.[223]

En canvi, s'ha observat que hi ha altres actors no estatals nacionals i internacionals en les dinàmiques de vigilància massiva dirigida a la societat libanesa. Destaca el cas del programari maliciós[224] conegut com a Flame, provinent de l'Iran, que l'any 2012 es va utilitzar per piratejar mòbils i ordinadors, o l'ús del programari maliciós Zoopark entre el 2015 i el 2018, amb capacitat per obtenir dades de missatges SMS, navegacions per internet, localització GPS i contrasenyes, entre altres. No obstant això, la principal bretxa de seguretat al país ha estat el recent atac massiu d'Israel, que ha fet explotar els dispositius cercapersones i walkie-talkies de militants de Hezbollah. L'atemptat va deixar 32 morts, incloent-hi nens i milers de persones ferides per tot el país.[225]

2. CONTROL DE LA LLIBERTAT D'EXPRESSIÓ EN LES ESFERES DIGITALS

Des de les protestes del 2019, l'emergència de mitjans alternatius de comunicació ha estat una tendència creixent. Nombroses blogueres i mitjans digitals independents han creat formes de comunicació més properes a la societat. Un dels exemples clau va ser la retransmissió en directe, amb històries i testimonis a peu de carrer durant l'explosió al port de Beirut, al 4 d'agost de 2020. Les noves blogueres i mitjans independents fan servir xarxes socials i blogs per difondre els seus materials. Per tal

221 **Abed Kataya.** "How Did Hackers Hijack Beirut Airport's Screens?" SMEX. 10 de gener del 2014. Disponible a: 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 gener del 2024. Disponible a: 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 setembre del 2024.

224 Vegeu glossari

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

de silenciar aquestes veus dissidents, el Govern monitora els continguts dels espais digitals.

Des del 2006, l'Ofiicina de Ciberdelinqüència i Drets de la Propietat Intel·lectual, adjunta al Departament d'Investigacions Criminals Especials de l'ISF, és l'encarregada de perseguir els delictes que utilitzen les tecnologies de la informació. Aquesta oficina ha estat denunciada per les seves pràctiques de censura i abusos sobre l'exercici de la llibertat d'expressió i premsa de periodistes, blogueres i altres figures públiques del país.[226] La vigilància i persecució de periodistes i blogueres s'efectua a través dels articles sobre difamació del Codi Penal (art. 582-582, 383,386) i la Llei de publicacions (art. 20-21). Segons les dades oficials, entre el gener del 2019 i el març del 2024, l'Oficina de Ciberdelinqüència va investigar 1684 casos de difamació.[227]

Al Líban, les detencions, els interrogatoris i les intimidacions de defensores de drets humans són una pràctica habitual.[228] Segons la fundació Samir Kassir, des del 2018 s'han registrat més de 800 abusos a periodistes com ara interrogatoris, coaccions, assetjament per telèfon i violència física per part de les Forces de Seguretat de l'Estat.[229] Alguns casos rellevants van ser el del periodista Jean Kassir, del mitjà digital Megaphone, el 2013, que va ser detingut i interrogat per les ISF, acusat de difamació per les seves crítiques als líders polítics, pel cas de l'explosió al port de Beirut.[230] Aquell mateix any, Lara Bitar, del mitjà digital The Public Source va ser convocada per l'Oficina per publicar un article sobre residus tòxics al Líban.[231] Altres fonts denuncien pràctiques de coacció com amenaces d'enviament de programari maliciós[232] per controlar l'activitat de les defensores de drets humans a les xarxes socials.[233] Acces Now també informa de casos de coacció per forçar a

226 **Amnistia Internacional.** "Lebanon: End Use of Defamation Laws to Target Journalists and Critics." 3 de maig del 2024.
Disponible a:
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 març del 2012.
Disponible a:
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 d'abril del 2023.
Disponible a:
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 d'abril del 2023.
Disponible a: 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 a: https://smex.org/lebanon-summoning-journalists-in-beirut-and-silencing-voices-in-mount-lebanon/

232 Vegeu glossari

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

defensores de drets humans a cessar les seves activitats en línia, a través de la signatura d'un document de compromís.[234]

En aquest sentit, Imad Bazzi apunta que la pràctica comuna no és el monitoreig exhaustiu de les xarxes socials per identificar continguts "inapropiats", sinó més aviat un procés on les elits que se senten "molestes" per l'activisme polític d'una persona, es posen en contacte amb un partit polític per activar una persecució legal, a través de la fiscalia de l'Estat o bé posar en marxa els mecanismes de l'Oficina de Ciberdelinqüència.[235] En la majoria dels casos, aquestes campanyes no es fan públiques i les persones defensores de drets humans simplement desapareixen de l'escena pública o s'autocensuren.[236]

L'Oficina de Ciberdelinqüència compta amb nombrosos recursos i tecnologia per monitorar les xarxes socials i piratejar telèfons mòbils. En aquest sentit, el 2015 es va detectar una proposta de contracte entre l'empresa Hacking Team i l'Oficina, per un valor de 450 000 dòlars,[237] per suposadament ciberespiar 50 persones. L'any 2013, el centre Citizen Lab va informar de la presència de la tecnologia PacketShaper de l'empresa Blue Coat per monitorar les interaccions d'usuàries de les xarxes socials, missatgeria i comunicacions en línia.[238] Arran d'aquest monitoreig de l'espai digital, el Govern va procedir a bloquejar webs, blogs i aplicacions. L'any 2015, SMEX va identificar el tancament de 45 pàgines web vinculades amb Israel, cases d'apostes, pornografia, prostitució, però també col·lectius LGBTIQ+.[239] El 2018, el Ministeri de Telecomunicacions va bloquejar la plataforma per a la creació del web Wix[240] i el 2020, el web de creació de blogs Blogger (*.blogspot.com). En una línia similar, el 2019, l'aplicació de cites Grindr també va ser bloquejada, sense cap tipus d'informació

234 **Access Now.** "When Cybercrime Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA". 13 de gener del 2023.
Disponible a:
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 setembre del 2024.

236 Ibid.

237 **SMEX.** "HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices". 30 de juliol del 2015.
Disponible a:
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 de gener del 2013. Disponible a:
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 març del 2015.
Disponible a: https://smex.org/mapping-blocked-websites-in-lebanon-2015/

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

ni justificació del Ministeri de Telecomunicacions.[241] La situació, mes que no pas millorar, apunta a un enduriment de les penes. La nova proposta de Llei per a mitjans de comunicació inclou penes de fins a tres anys per difamar les religions reconegudes al país.[242] Davant d'aquesta situació, Amnistia Internacional va iniciar una campanya l'any 2023 per reformar les lleis sobre difamació al Líban sota el hashtag #MyOpinionIsNotaCrime.[243]

3. DE LA VIGILÀNCIA A LES XARXES SOCIALS A LA VIOLÈNCIA DIGITAL

La vigilància policial contra les persones queer s'ha identificat, des del 2018. Aquesta persecució combina la vigilància massiva de les esferes digitals amb la identificació de persones LGBTIQ+ a les vies públiques de les principals ciutats del país. L'article 542 del Codi Penal libanès criminalitza les relacions entre persones del mateix sexe.[244] Aquesta criminalització es tradueix en la vigilància i l'assetjament en línia d'aquests col·lectius. L'organització britànica Article 19 assegura que les ISF fan servir les aplicacions de cites Grindr, Hornet, PlanetRomeo i Growl per recollir evidències de conductes homosexuals per arrestar i denunciar posteriorment a aquestes persones.[245] A aquest assetjament en línia, s'hi suma la identificació de persones LGBTIQ+ a la via pública per confiscar i examinar els seus telèfons mòbils, amb l'objectiu de trobar imatges i informacions a la biblioteca de fotos o xats de WhatsApp, per part de la policia, per ser utilitzades posteriorment en processos de denúncia.[246]

241 **SMEX.** "The Case of the Blocked Blogger: How the MoT Continues to Violate Free Expression in Lebanon". 3 de gener del 2020.
Disponible a:
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 novembre del 2023.
Disponible a:
https://english.legal-agenda.com/proposed-media-law-poses-grave-threat-to-freedom-of-expression/

243 **Amnistia Internacional.** "Campaign to Decriminalize Defamation and Insult in Lebanese Laws". 8 d'agost del 2023.
Disponible a:
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 juliol del 2018.
Disponible a: 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 a:
https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf

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

"Les elits polítiques del país disposen d'exèrcits electrònics formats per milers de bots, per desenvolupar campanyes massives de desinformació i assetjament en línia i, d'aquesta manera, atacar la reputació d'un col·lectiu o persona"

Aquestes pràctiques que duen a terme les forces de seguretat de l'Estat, en què es requisen mòbils, ordinadors i altres dispositius de comunicació, i que han augmentat des de les manifestacions del 2019, també es produeixen en camps de refugiats sirians, fet que accentua l'aïllament social d'aquestes comunitats.[247] Aquest tipus de pràctiques realitzades per les Forces de Seguretat de l'Estat ha augmentat des de les manifestacions del 2019. L'organització SMEX indica que no hi ha cap marc legal clar en aquest sentit.[248]

La criminalització i l'assetjament físic de col·lectius LGBTIQ+ o de les persones refugiades es justifica a través de campanyes de desinformació i assetjament en línia. Per exemple, des de mitjan 2024, han augmentat els discursos d'odi a les xarxes socials i els mitjans de comunicació contra les persones refugiades sirianes per part del Govern libanès, líders polítics, religiosos, i fins i tot de grups afins a Hezbollah.[249] L'analista digital, Ralph Baydoun detalla que les elits polítiques del país disposen d'exèrcits electrònics[250] formats per milers de bots, per desenvolupar campanyes massives de desinformació i assetjament en línia i, d'aquesta manera, atacar la reputació d'un col·lectiu o persona.[251]

Aquests atacs contra la reputació perpetrats a les xarxes, també es traslladen als espais físics i inclouen agressions i assassinats. Un dels casos més paradigmàtics, relacionat amb la denúncia de casos de corrupció del Govern el 2019, va tenir greus implicacions laborals i per a la integritat física i psicològica de la periodista implicada i dels seus familiars.[252] Es van endegar campanyes de violència digital i *lawfare*, incitació a l'odi i dòxing.[253] El cas també va derivar en una sentència judicial d'un any de presó per aquesta dona defensora per una causa de difamació, després que denunciés públicament la violència

247 **ACHR.** "Lebanon: Censorship and Violations of Free Speech". Arab Center for Human Rights. 13 de gener del 2023. Disponible a: 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 a: 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 d'agost del 2024.
Disponible a:
https://timep.org/2024/08/28/targeted-how-misinformation-puts-lebanons-syrian-refugees-in-danger/

250 Vegeu glossari

251 Ralph Baydoun, entrevista personal realitzada per l'equip d'investigació, 6 de setembre del 2024.

252 Per raons de seguretat de la persona defensora, se n'omet el nom així com les referències del cas.

253 Vegeu glossari

contra defensores de drets humans exercida per membres del partit cristià Free Patriotic Movement. Les dones es veuen especialment afectades per la violència digital. Segons SMEX, entre el 2020 i el 2023, el 80 % dels objectius de la violència digital al Líban eren dones.[254]

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

VI

LA GUERRA DE SÍRIA EXACERBA LA VIGILÀNCIA MASSIVA

El ciberespai a Síria està fortament regulat i controlat pel Govern, a través de diversos ministeris i entitats. Aquesta activitat es va començar a produir de manera més intensa, a partir dels esdeveniments que van tenir lloc durant la Primavera Àrab. L'aparell de seguretat del Govern sirià està conformat per la intel·ligència militar siriana, on diferents unitats col·laboren per exercir control i vigilància cibernètica sobre la població. En aquest sentit, la Unitat 225 és la responsable de monitorar les comunicacions internes.[255] Aquesta unitat té la capacitat per bloquejar números específics, finalitzar trucades o deshabilitar missatges SMS,[256] entre d'altres. També hi ha la unitat 211,[257] coneguda com la branca "tècnica" o "informàtica", que se centra en la regulació de l'accés a llocs web, gestiona les comunicacions sense fils i dona suport tècnica a la Unitat 225. Finalment, la Unitat 237[258] està especialitzada en el seguiment i intervenció de trucades sense fil.

"El ciberespai a Síria està fortament regulat i controlat pel Govern, a través de diversos ministeris i entitats, de manera més intensa a partir dels esdeveniments que van tenir lloc durant la Primavera Àrab"

Quan es van iniciar les protestes a generalitzades a la regió del Maghreb i Mashreq, especialment a Egipte i a Tunísia, el president sirià Assad va deduir que les protestes havien aconseguit derrocar els seus líders perquè els Governs no van reprimir les manifestacions amb prou antelació. El Govern d'Assad ja era conegut abans de la guerra per censurar el contingut d'internet al país.[259] Tan bon punt van començar les protestes, el president sirià Assad va expulsar a les periodistes estrangeres del país per controlar la cobertura

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. Maig del 2017. Disponible a: 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 a: https://dergipark.org.tr/en/download/article-file/3842663

257 **Syrian Network for Human Rights.** "Syrian Security Branches and Persons in Charge." Disponible a: 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 a: 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 a: https://www.jstor.org/stable/10.7249/j.ctt4cgd90

periodística dels esdeveniments i l'ús que feien d'internet.[260] Els diferents proveïdors d'internet a Síria operen sota la l'Empresa Telecomunicacions de Síria (STE), propietat del Govern. L'STE, establerta el 1975, és fonamental en el domini cibernètic de Síria i proporciona connectivitat global i regula el flux d'informació. Així mateix, en nombroses ocasions, el Govern sirià va bloquejar internet i la telefonia mòbil durant diversos dies per impedir, entre altres, que les manifestants publiquessin vídeos, imatges o comentaris sobre els esdeveniments a les xarxes socials.[261]

"En aquest marc de vulneracions sistemàtiques de drets és on, l'abril del 2022, es va introduir la nova Llei siriana de ciberseguretat, que s'ha convertit de facto en part de les tàctiques legals repressives imposades pel règim sirià per criminalitzar la llibertat d'expressió i el lliure flux d'informació, amb el pretext de combatre la ciberdelinqüència"

Una dècada després que Assad reprimís les manifestacions de la població siriana, el règim segueix consolidant el seu poder i criminalitza la llibertat d'expressió alhora que redueix els espais cívics per reprimir qualsevol forma de dissidència o oposició. En aquest marc de vulneracions sistemàtiques de drets és on, l'abril del 2022, es va introduir la nova Llei siriana de ciberseguretat,[262] que s'ha convertit de facto en part de les tàctiques legals repressives imposades pel règim sirià per criminalitzar la llibertat d'expressió i el lliure flux d'informació, amb el pretext de combatre la ciberdelinqüència¨.

260 **Hossain, M.** The impact of cyber capabilities in the Syrian civil war. 2020. Small Wars Journal. 2016. Disponible a: 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 novembre del 2012.
Disponible a:
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 a: https://www.indexoncensorship.org/2022/05/syria-passes-draconian-cybercrime-laws/

1. LA REPRESSIÓ DE LES DISSIDÈNCIES POLÍTIQUES A TRAVÉS DELS EXÈRCITS ELECTRÒNICS263

La llibertat d'expressió està subjecta a un estricte control a tota Síria. El règim ha incrementat recentment la seva ja estricta legislació, amb l'aprovació l'abril del 2022, d'un nou decret llei sobre ciberdelinqüència,[264] que imposa dures penes per a qualsevol activitat en línia que soscavi el "prestigi de l'Estat" o la "unitat nacional", entre altres disposicions vagues. Un dels punts clau d'aquesta nova Llei és el control que pretén aplicar sobre allò que descriu com *fake news*[265] o notícies falses que puguin arribar a soscavar el prestigi de l'Estat o perjudicar la unitat nacional. Aquest delicte comporta una pena privativa de llibertat de fins a 5 anys i sancions econòmiques quantioses. Segons Syrian Network for Human Rights (SNHR), les conseqüències de l'entrada en vigor d'aquesta Llei en el marc jurídic sirià han estat nefastes per a la població civil, especialment per a col·lectius d'activistes, defensores de drets humans i opositores al règim. Com a mínim una persona ha mort com a conseqüència de les tortures i 146 persones han estat arrestades de manera arbitrària dins d'aquest nou marc legal.[266]

"El passat mes de juny del 2024, la SNHR va publicar un informe on analitza una altra llei més recent sobre la creació d'un Ministeri de Mitjans de Comunicació. Segons l'SNHR, aquesta llei és un instrument per consolidar el control del règim sobre el contingut dels mitjans de comunicació, imposar més censura contra la premsa privada i les publicacions que entren al país i imposar més restriccions a la producció televisiva."

El passat mes de juny del 2024, la SNHR va publicar un informe on analitza una altra llei més recent sobre la creació d'un Ministeri de Mitjans de Comunicació.[267] Segons l'SNHR, aquesta llei és un instrument per consolidar el control del règim sobre el contingut dels

263 Vegeu glossari

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

265 Vegeu glossari

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. 2014." Disponible a: 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

mitjans de comunicació, imposar més censura contra la premsa privada i les publicacions que entren al país i imposar més restriccions a la producció televisiva. En aquest sentit, entre el març del 2011 i el maig del 2024, l'SNHR va documentar l'assassinat de 717 periodistes.[268]

Abans que es promulgués aquesta Llei, hi havia hagut diversos grups de pirates informàtics que van donar suport digital al règim d'Assad durant el conflicte. En aquest sentit, l'any 2016, es va publicar una investigació sobre Group 5,[269] un col·lectiu de pirates informàtics pro iranià que donava suport al règim d'Assad. Aquest grup de hackers va crear pàgines web amb noms com AssadCrimes, com a part dels seus elaborats esquemes d'enginyeria informàtica per fer caure a la trampa membres de l'oposició i defensores de drets humans que, quan clicaven a l'enllaç, estaven habilitant l'accés a tota la informació dels seus ordinadors.

Un altre grup de pirates o hackers que ha donat suport a Assad és Syrian Electronic Army (SEA).[270] El SEA opera amb el suport del règim i utilitza atacs DDoS,[271] estafes de *phishing*[272] o pesca i altres trucs, per vigilar persones defensores de drets humans i opositores al règim, així com els mitjans de comunicació crítics. Una investigació del 2013 va demostrar que el nom del domini del lloc web del grup l'havia registrat la Societat de Computació de Síria (SCS), una organització que havia estat dirigida pel president sirià Bashar A-Assad l'any 1995, abans que assumís la presidència.[273] Dins d'aquest grup hi hauria un subgrup anomenat The Syrian Malware Team (SMT), que feia servir tecnologia RAT (Remote Accés Tool o eina d'accés remot) per entrar als dispositius mòbils i accedir a tota la informació que hi contenien.[274] Així i tot, no està clar si els membres d'aquests grups tenen un vincle directe amb Govern sirià o simplement són un grup de pirates informàtics pro Assad.

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

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

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

271 Vegeu glossari

272 Vegeu glossari

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

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

2. CENSURA I CONTROL DE LES TELECOMUNICACIONS A L'ESPAI DIGITALITZACIÓ

El Govern sirià va posar en marxa el seu primer sistema de monitoreig de xarxes a escala nacional, el 1999. El sistema, encarregat per l'empresa de telecomunicacions siriana Syrian Telecom (STE) va ser dissenyat per monitorar la telefonia mòbil, fixa i internet. Actualment, els atacs cibernètics són comuns i el control d'Internet s'utilitza com una arma de guerra: hi ha apagades intencionades freqüents, que es fan servir per desactivar temporalment les xarxes de comunicació establertes per grups contraris al règim. Immediatament després de l'aixecament del 2011, el règim sirià va tancar tots els accessos a internet a l'est de Síria i hi va haver apagades intermitents que han seguit durant tot el conflicte, a més de restringir completament contingut en pàgines web que cobrien temes que el règim considerava sensibles. [275]

"Actualment, els atacs cibernètics són comuns i el control d'Internet s'utilitza com una arma de guerra: hi ha apagades intencionades freqüents, que es fan servir per desactivar temporalment les xarxes de comunicació establertes per grups contraris al règim."

Uns anys abans de les revoltes àrabs, el Govern sirià va construir sistemes de monitoreig de comunicacions, a través de diversos projectes, on va ser essencial el coneixement i l'experiència d'algunes empreses del Nord Global. En aquest sentit, empreses com VASTech (Sudàfrica) i AGT (Emirats Àrabs Units – Alemanya) van contribuir, en gran mesura, a l'estat repressiu de vigilància de Siria, amb solucions de control, vigilància i censura a les xarxes.[276]

Durant l'inici del conflicte sirià, el Govern va utilitzar dispositius de monitoreig de telecomunicacions de l'empresa Blue Coat Systems, amb seu als Estats Units, per al filtratge de xarxes, la censura i la vigilància. Malgrat les sancions dels Estats Units, que prohibeixen les vendes a Síria, aquests dispositius es van enviar a un distribuïdor de Dubai per, posteriorment, ser enviats a Síria.[277]

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

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

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

Hi va haver altres empreses occidentals que van establir vincles amb el règim d'Assad i li van distribuir tecnologia de vigilància digital. Una d'aquestes empreses és la italiana Area SpA,[278] que ven sistemes de monitoreig capaços de capturar el trànsit d'internet, interceptar converses i rastrejar objectius, a través de GPS i que va obtenir contractes amb els Governs de Síria i Egipte.[279] La companyia italiana hauria començat a instal·lar sistemes de monitoreig de xarxes que dotarien el Govern sirià de capacitat per interceptar, escanejar i catalogar pràcticament tots els correus electrònics que circulen pel país, així com rastrejar objectius i cartografiar les xarxes de contactes de la població siriana.

Una de les empreses que també va facilitar la posada en marxa d'una estructura de vigilància digital a Síria és l'empresa alemanya Utimaco.[280] Segons informacions de l'European Center for Constitutional and Human Rights (ECCHR), Ultimaco va participar juntament amb Area SpA d'un sistema de vigilància administrat per Syrian Telecom (STE).[281] El gener del 2018, l'ECCHR va presentar una denúncia penal davant la Fiscalia Federal Alemanya contra aquesta empresa, per la seva presumpta complicitat en crims de lesa humanitat i crims de guerra. L'empresa francesa Qosmos també va ser denunciada davant d'un tribunal francès, per organitzacions de la societat civil que l'acusaven de proporcionar al Govern sirià programari d'inspecció profunda de paquets (DPI),[282] que va permetre al règim rastrejar defensores de drets humans,[283] dissidents i membres de l'oposició, alguns dels quals van acabar essent torturats o executats, després que comencés l'aixecament inicial contra el règim, l'any 2011.[284]

Els membres de la societat civil siriana saben perfectament que les seves comunicacions estan essent vigilades i prenen mesures al respecte. Segons comparteix Abdulaziz Rama-

278 **Privacy International.** "Building Syria's Surveillance State". 2016.
Disponible a: 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 a:
https://www.vice.com/en/article/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria/

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

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

282 Vegeu glossari

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

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

dan,[285] director executiu de DOZ e.V.[286] "acordem determinats nivells de seguretat de com compartir la informació en plataformes com WhatsApp". "Hem de pensar en noves eines que ens permetin no sentir-nos amenaçats i exercir lliurement el nostre dret fonamental a la llibertat d'expressió".

3. VIGILÀNCIA MASSIVA I CONTROL DE L'ACTIVISME A LA DIÀSPORA: EL PAPER DE LES MISSIONS DIPLOMÀTIQUES

Després de la repressió sistemàtica durant la Primavera Àrab i, més encara, durant la guerra de Síria, milers de dones defensores dels drets humans van fugir del país. No obstant això, el règim sirià va continuar la persecució més enllà de les seves fronteres.[287] Una investigació del Centre de Justícia i Responsabilitat de Síria (SJAC, per les seves sigles en anglès) va revelar documents que demostraven que la vigilància a l'estranger de la societat civil siriana es duia a terme sistemàticament a tota la xarxa de missions diplomàtiques del règim.[288] Entre el 2013 i el 2015, el SJAC va poder accedir a aproximadament 483 000 pàgines de documents classificats d'instal·lacions estatals sirianes abandonades. Gràcies a aquesta documentació, el SJAC va descobrir que la vigilància sobre la societat civil siriana es produïa en llocs tan diferents com Espanya, Bielorússia, Bèlgica, Xipre, Egipte, França, Grècia, l'Iraq, el Japó, Jordània, Líban, Rússia, l'Aràbia Saudita, Turquia, Ucraïna, Regne Unit i Iemen. Aquests documents, els havien emès diferents agències d'intel·ligència que depenien del Ministeri de l'Interior i el Ministeri de Defensa. Aquestes pràctiques de vigilància i control de la societat civil siriana s'han donat també a l'Estat espanyol, on

"Una investigació del Centre de Justícia i Responsabilitat de Síria (SJAC, per les seves sigles en anglès) va revelar documents que demostraven que la vigilància a l'estranger de la societat civil siriana es duia a terme sistemàticament a tota la xarxa de missions diplomàtiques del règim"

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

286 Organización de la sociedad civil Síria con sede en Alemania.

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

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

grups d'opositors al règim sirià van protestar davant l'ambaixada de Síria a Madrid en determinades ocasions.

Segons la informació obtinguda per Amnistia Internacional,[289] el mateix personal de l'ambaixada on es van produir les protestes fotografiava i enregistrava vídeos per identificar les participants. Posteriorment, aquest material s'enviava al *Mukhabarat*[290] (servei d'intel·ligència sirià) i des d'allà, s'identificava cadascuna de les persones participants i es prenien mesures en contra d'elles i dels seus familiars. Entre les conseqüències a què s'enfrontaven les persones que participaven en aquestes protestes, hi havia l'obstaculització de procediments administratius que havien de dur a terme a l'ambaixada.[291] Al mateix temps, aquestes pràctiques legítimes de protesta es converteixen en l'excusa perfecta del règim sirià per acoquinar, amenaçar, arrestar i fins i tot colpejar a familiars i éssers estimats que la comunitat opositora siriana a l'estranger encara té al país.[292]

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

290 Mukhabarat, que en àrab vol dir intel·ligència, és un terme general per a les agències d'intel·ligència, en el cas de Siria, Intel·ligència General (també coneguda com a Seguretat de l'Estat), Intel·ligència Militar, Intel·ligència de la Força Aèria i Seguretat Política. **Amnistia Internacional.** "Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home." Índex MDE 24/057/2011. 3 d'octubre del 2011.
Disponible a: https://www.amnesty.org/en/documents/mde24/057/2011/en/.

291 **Amnistia 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 d'octubre del 2011.
Disponible a: https://www.amnesty.org/en/documents/mde24/057/2011/en/

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

4. CONTROL SOBRE LA COMUNITAT KURDA AL NORD-EST DE SIRIA

L'any 2022, el SJAC va publicar un informe,[293] després d'analitzar documentació sensible abandonada pel Govern sirià, que evidencia la persecució contra la població kurda. El SJAC va identificar un total de 349 pàgines que esmentaven persones o activitats kurdes, fet que queda reflectit en pràctiques repressives sistemàtiques que atempten contra els drets humans. Algunes de les mesures que s'han utilitzat per a la persecució de la comunitat kurda i que s'han descobert gràcies a la investigació del SJAC són:[294]

- Violació de la llibertat de reunió i d'expressió. Diverses pàgines convidaven l'aparell de seguretat sirià a interrompre directament les protestes planificades i a requerir més permisos específics per permetre reunions públiques de grups kurds.
- Violació dels drets culturals. Dues de les pàgines analitzades transmetien el temor que l'expressió de la cultura i la llengua kurdes suposessin una amenaça per a la unitat siriana. Com a resposta a l'augment de les activitats polítiques kurdes, una pàgina descrivia el pla del Govern per criminalitzar totes les activitats "nacionalistes" kurdes,
- Supervisió de la propietat i l'economia kurda. Els documents també indicaven el temor de l'accés kurd a la terra i la riquesa. Algunes pàgines recomanaven que els municipis exigissin permisos, abans de comprar o vendre terres, que es vigilessin de prop els patrons de compra de la comunitat kurda i que se la castigués per participar en transaccions immobiliàries no autoritzades.
- Diluir la composició ètnica de les zones kurdes. Una de les pàgines convidava les forces estatals sirianes a pressionar les tribus àrabs perquè es traslladessin a la província de Hassakeh, pel que sembla, per diluir la majoria kurda. Una altra pàgina recomanava específicament evitar que el kurd fos el grup ètnic majoritari, a qualsevol regió.
- Persuasió i intimidació de líders kurdes. Els documents ordenaven específicament que les líders kurdes fossin cooptades i que es prenguessin mesures per encoratjar les persones a identificar-se més com a sirianes. Tot això, a través de mitjans de persuasió i intimidació per atraure i amenaçar les líders kurdes perquè s'alineessin amb el Govern.

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

294 Ibid.

"Des de l'any 2019, a les xarxes hi ha hagut diverses campanyes d'espionatge digital dirigides contra la comunitat kurda"

"A través de perfils falsos de Facebook que invitaven a descarregar aplicacions d'Android, s'activava un virus troià d'accés remot que permetia accedir al registre de trucades, consultar i exportar arxius i fer fotografies, entre altres coses. "

A més, com a mínim des de l'any 2019, a les xarxes hi ha hagut diverses campanyes d'espionatge digital dirigides contra la comunitat kurda. En aquest sentit, l'empresa de ciberseguretat ESET i el centre d'intel·ligència xinès QiAnXin Threat Intelligence Center van descobrir l'any 2020[295] que a través de perfils falsos de Facebook que invitaven a descarregar aplicacions d'Android,[296] s'activava un virus troià d'accés remot[297] que permetia accedir al registre de trucades, consultar i exportar arxius i fer fotografies, entre altres coses.

295 **Stone, J.** "Spyware APP Designed to Monitor Kurdish." CyberScoop. 8 de setembre del 2021. Disponible a: https://cyberscoop.com/spyware-kurds-eset-bladehawk-iran/.

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

297 Vegeu glossari

VII

TESTED IN SURVEILLANCE: PALESTINA COM A CAMP DE PROVES DE L'ESTAT D'ISRAEL

La vigilància militar israeliana sobre el poble palestí té una llarga història que es remunta a la fundació de l'Estat d'Israel en terres palestines, el 1948, moment en què 750 000 persones palestines van ser expulsades de casa seva i Israel va sotmetre a qui es va quedar a un govern militar, marcat per una vigilància generalitzada.[298] És en aquest marc de vulneracions sistemàtiques, que les empreses de ciberseguretat formen part d'una xarxa de vigilància cada vegada més gran, que està afermant el control del Govern d'Israel sobre la població palestina i que, a més, ajuda a mantenir el sistema d'apartheid israelià.[299]

"La llibertat de desenvolupar tot tipus de tecnologia armamentística i de seguretat, per després posar-la a prova sobre la població palestina, va permetre que, a principis del segle XXI, Israel emergís com a líder mundial en tecnologies de vigilància, tendència que s'ha mantingut en el temps i que sembla que no es veu afectada per l'actual genocidi a Gaza"

La llibertat de desenvolupar tot tipus de tecnologia armamentística i de seguretat, per després posar-la a prova sobre la població palestina, va permetre que, a principis del segle XXI, Israel emergís com a líder mundial en tecnologies de vigilància, tendència que s'ha mantingut en el temps i que sembla que no es veu afectada per l'actual genocidi a Gaza.[300] De fet, l'exèrcit d'Israel (IDF, per les seves sigles en anglès) és la principal incubadora de *startups* de ciberseguretat del món. El servei militar en general i, concretament, la Unitat d'Intel·ligència i Ciberseguretat 8200 de l'exèrcit israelià serveixen com autèntiques experiències professionals per als joves militars, abans d'incorporar-se al sector privat de la ciberseguretat.[301] No sorprèn doncs que un estudi del 2018 citat pel diari israelià Haaretz estimés que el 80 % de les 2300 persones que van fundar les 700 empreses de ciberseguretat d'Israel havien passat per aquesta Unitat d'Intel·ligència de l'exèrcit israelià.[302]

Durant les revoltes àrabs, plataformes com Facebook, Instagram i TikTok van ser part integral de les protestes generalitzades a tota la regió Mashreq, inclosa Palestina. En aquest sentit, l'Estat d'Israel va instaurar un control ferri de les xarxes socials i es va tornar un

298 **Institute for Middle East Understanding.** "Quick facts: Palestinian Refugees" 19 de juny del 2024. Disponible a: https://imeu.org/article/quick-facts-palestinian-refugees

299 **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 març del 2022. Disponible a: https://www.ohchr.org/en/press-releases/2022/03/israels-55-year-occupation-palestinian-territory-apartheid-un-human-rights

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

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

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

element clau en la vigilància i la posterior repressió de la població palestina.[303] Més tard, en el marc de la COVID-19, Israel va posar en pràctica una sèrie de mesures legals que justificaven l'expansió dels sistemes de vigilància i de les tecnologies de control.[304] De fet, la pandèmia de la COVID-19 va contribuir a normalitzar i legitimar els abusos de poder i les violacions de drets humans comeses per les forces de seguretat de l'Estat d'Israel en connivència amb les empreses de ciberseguretat que desenvolupen i posen en pràctica aquestes tecnologies.[305] Una d'aquestes empreses és NSO Group, que el març del 2020 va llançar un software de rastreig de contactes anomenat Fleming.[306] Més recentment, mesos abans de la invasió de Gaza, l'Estat d'Israel va aprovar una llei coneguda per l'oposició com "Big Brother in Public Spaces" (El gran germà als espais públics) amb què es promou i es regula l'ús de sistemes biomètrics a l'espai públic, inclús per part de la policia d'Israel. EL projecte de llei inclou implicacions de gran abast en relació amb el dret a la privacitat. El sistema que es pretén implementar permetria processar fotografies de persones per comparar-les amb una base de dades.[307] [308]

1. GENOCIDI I ÚS D'EINES D'INTEL·LIGÈNCIA ARTIFICIAL

Israel manté un bloqueig a la Franja de Gaza per terra, mar i aire, des de fa 17 anys. L'octubre del 2023, Israel va iniciar una nova invasió del territori i va marcar l'inici del genocidi actual sobre la població palestina. Paral·lelament, l'exèrcit d'Israel i colons armats han

303 **7amleh.** "Israel's Surveillance Industry and Human Rights." Desembre del 2023.
Disponible a: https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

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

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

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

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

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

endegat una campanya d'atacs sistemàtics contra la població de Cisjordània. Aquests atacs han propiciat una escalada en les pràctiques de control i vigilància sobre la població palestina. El fet nou d'aquesta nova onada de violència i repressió de la població palestina és l'ús d'eines d'intel·ligència artificial (IA).

"El fet nou d'aquesta nova onada de violència i repressió de la població palestina és l'ús d'eines d'intel·ligència artificial (IA)"

Així doncs, l'exèrcit d'Israel ha desenvolupat un programa basat en intel·ligència artificial[309] conegut com a "Lavender" i "Gospel".[310] Segons alguns oficials de les unitats d'intel·ligència israelianes que han participat de primera mà en l'ús de la IA a Gaza, Lavender ha tingut un paper clau en el bombardeig de la població civil palestina, especialment durant les primeres etapes de la guerra.[311] Hi ha una altra eina anomenada "*Where is Daddy*?" (On és el papa?) que s'afegeix a la utilització d'aquests sistemes automatitzats de generació d'objectius humans i objectius d'infraestructura com Lavender i Gospel. Es tracta d'un sistema d'intel·ligència artificial dissenyat per rastrejar i seleccionar presumptes militars de Hamás quan són a casa amb les seves famílies.[312]

Un altre tipus d'eines de la IA que s'han fet servir en els atacs contra la Franja de Gaza són els sistemes d'armes autònomes letals (LAWS, per les seves sigles en anglès) i armes semi autònomes (semi-LAWS).[313] L'exèrcit israelià ha estat pioner en l'ús de quadricòpters amb control remot, equipats amb metralladores i míssils per vigilar, controlar i atacar persones i infraestructures.[314] Israel ha estat classificat com el principal proveïdor de drons

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

310 **Yuval, A.** "A mass assassination factory." +972 Magazine. 30 de novembre del 2023.
Disponible a: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

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

312 **Democracy Now!** "Israel's AI Surveillance System for Palestinians". 5 d'abril del 2024.
Disponible a: https://www.democracynow.org/2024/4/5/israel_ai

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

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

suïcides del món.[315] Totes dues tecnologies han estat desenvolupades per Israel Aerospace Industries (IAI).[316]

Una de les empreses involucrades en l'actual genocidi de Gaza és el fabricant d'armes més gran d'Israel, Elbit Systems, principal proveïdor de l'exèrcit israelià. Actualment el 85 % de totes les armes, sistemes de vigilància i eines que utilitza l'exèrcit israelià han estat fabricades per Elbit, inclosos els drons militars Skylark i Hermes, que formen la majoria de la flota de grans avions no tripulats d'Israel i que s'han utilitzat àmpliament a Gaza. En molts casos, l'ús d'aquest tipus d'eines té com a conseqüència la mort de civils i planteja qüestions relatives a les possibles violacions del Dret Internacional Humanitari (DIH), entre les quals hi ha el principi de distinció, pel qual cal complir el requisit de distingir estrictament entre objectius civils i militars.[317] [318]

"La creixent onada violenta a Cisjordània i Jerusalem Aquest i el genocidi a Gaza ha propiciat l'aparició d'una nova tendència de defensa civil i de resistència a l'ocupació. Periodistes, blogueres, creadores de contingut i influencers palestines mostren el dia a dia de les violacions de drets humans perpetrades per Israel a Gaza i a la Cisjordània ocupada, mentre veuen perillar la seva feina i la seva vida."

La creixent onada violenta a Cisjordània i Jerusalem Aquest i el genocidi a Gaza ha propiciat l'aparició d'una nova tendència de defensa civil i de resistència a l'ocupació.[319] Periodistes, blogueres, creadores de contingut i influencers palestines mostren el dia a dia de les violacions de drets humans perpetrades per Israel a Gaza i a la Cisjordània ocupada, mentre veuen perillar la seva feina i la seva vida. El col·lectiu de treballadores de mitjans de comunicació i periodistes ha estat un dels col·lectius objectiu de la guerra a Gaza, per part d'Israel.[320] A finals de setembre del 2023, 128 periodistes i personal de mitjans de

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

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

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

318 **Verfassungsblog.** "Gaza, Artificial Intelligence and Kill Lists." 16 de maig del 2024. Disponible a https://verfassungsblog.de/gaza-artificial-intelligence-and-kill-lists/

319 **El Salto Diario.** "Ciberactivismo." 29 de juny del 2024. Disponible a: https://www.elsaltodiario.com/analisis/digitine-ciberactivismo-movimiento-pro-palestina

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

comunicació havien estat assassinats a Gaza, segons el CPJ—*Committee to Protect Journalists*[321] (Comitè per Protegir Periodistes). Un dels casos paradigmàtics de l'assetjament i el control israelians sobre periodistes i influencers és el del palestí Motaz Azaiza,[322] de Gaza, que després de més de 100 dies documentant el genocidi de Gaza va haver de ser evacuat a Qatar, per raons de seguretat.[323] Un altre cas rellevant és el de Bisan Owda, periodista palestina, que recentment va rebre un premi per mostrar els atacs i la realitat del que passa a Gaza.[324]

2. SISTEMA DE RECONEIXEMENT FACIAL[325] I VIGILÀNCIA BIOMÈTRICA

"La invasió terrestre de Gaza per part d'Israel ha estat una oportunitat per a ampliar la vigilància biomètrica de les persones palestines, ja desplegada a Cisjordània i Jerusalem Est"

La invasió terrestre de Gaza per part d'Israel ha estat una oportunitat per a ampliar la vigilància biomètrica de les persones palestines, ja desplegada a Cisjordània i Jerusalem Est. El New York Times va informar sobre la manera com l'exèrcit israelià està utilitzant un ampli sistema de reconeixement facial a Gaza "per a dur-hi a terme una vigilància massiva i recollir i catalogar els rostres de les palestines sense el seu consentiment".[326] Segons aquesta informació, aquest sistema utilitza tecnologia de l'empresa israeliana Corsight i Google Photos per a seleccionar cares d'entre multituds i incloure-les en una base de dades. Corsight ha desenvolupat una aplicació de reconeixement facial basada en IA que és utilitzada per l'exèrcit israelià per a vigilar a la població palestina a Gaza.[327] A més, l'exèrcit

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

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

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

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

325 Vegeu glossari

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

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

israelià també ha establert punts de control, amb càmeres d'escaneig facial, al llarg de les principals carreteres que la població palestina estava fent servir per fugir de les zones on es produïen els atacs més intensos.[328] També s'està fent servir la tecnologia d'Alphabet, empresa subsidiària de Google, ja que l'exèrcit israelià utilitza la funció de reconeixement facial de Google Photos com a part de la vigilància i control total de la població palestina a Gaza. A més d'aquests serveis, Google ha ampliat la seva col·laboració amb el Ministeri de Defensa israelià, tot oferint-los un espai segur al núvol per processar i emmagatzemar tot tipus de dades.[329]

L'aïllament de Gaza no és només de caràcter tecnològic, sinó que també hi ha empreses que porten generant beneficis any rere any, gràcies a la construcció de tanques intel·ligents, és a dir, que inclouen sensors de moviment i tecnologia biomètrica i que separen Gaza de l'Estat d'Israel. Una de les empreses que hi tenen un paper clau és Magal Security.[330] Un altre dels contextos en què es pot recollir més informació, tant personal com biomètrica, és els *checkpoints* o punts de control militars, imposats per Israel. L'empresa Anyvision, rebatejada el 2021 com Oosto,[331] col·labora amb l'exèrcit israelià en un sistema instal·lat als punts de control militars israelians a la Cisjordània ocupada que utilitza la tecnologia de reconeixement facial[332] de la companyia per identificar permisos de treball. El setembre del 2020, Anyvision va acabar d'establir SightX, projecte que comparteix amb el fabricant d'armes israelià Rafael Advanced Defense Systems.[333] [334] SightX implementa tecnologies avançades de detecció i seguiment que utilitzen intel·ligència artificial i estan basades en la tecnologia de visió artificial desenvolupada per Anyvision, amb finalitats militars.[335]

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

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

330 **+972 Magazine.** "Israel arms companies that will profit from the last assault in Gaza". 2022.
Disponible a: https://www.972mag.com/israeli-arms-companies-surveillance-gaza

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

332 Vegeu glossari.

333 **Business and Human Rights Resource Center.** "Anyvision raises concerns". 28 de setembre del 2022.
Disponible a:
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

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

335 Ibid.

3. REPRESSIÓ TECNOLÒGICA I CONTROL DE LES COMUNICACIONS

L'espionatge sobre les defensores de drets humans és una tendència preocupant, que afecta directament al dret a la privacitat i al secret de les comunicacions, entre d'altres. En aquest sentit, al novembre del 2021, es va descobrir que com a mínim sis defensores de drets humans palestines, els havien piratejat el telèfon, a través del software Pegasus. Just després de la infiltració als dispositius de defensores de drets humans, el Govern d'Israel va incloure sis organitzacions no governamentals palestines que treballaven a Cisjordània a la llista d'organitzacions terroristes.[336]

Una altra tendència alarmant documentada és la detenció i interrogatori de palestines, per la seva activitat a les xarxes socials. Han sorgit nombrosos casos en què s'han detingut persones simplement per expressar els seus punts de vista o opinions en diverses plataformes digitals.[337] A més d'aquest control ferri de les xarxes socials, l'exèrcit israelià inspecciona de manera sistemàtica els telèfons mòbils de les palestines a Jerusalem Est i efectua sovint detencions arbitràries o assetjament.[338] Una defensora de drets humans palestina entrevistada recentment en el marc d'una trobada internacional compartia que "mentre faig servir el meu telèfon mòbil per parlar amb algú proper, sento veus d'altres persones i hem d'adaptar el llenguatge i adoptar capes de protecció de xifrat als nostres dispositius mòbils".[339]

Els bombardejos que es produeixen durant el genocidi actual han danyat la infraestructura de telecomunicacions i han provocat apagades totals i parcials a la Franja de Gaza. També han provocat deliberadament talls d'electricitat que han compromès encara més la connectivitat de tota la regió. Des de l'inici del genocidi, les autoritats israelianes han utilitzat les apagades d'internet com a eines de càstig col·lectiu, a través d'una sèrie de tàctiques, com ara la imposició d'apagades intermitents de les comunicacions que coincideixen amb intensos bombardejos, la destrucció de la infraestructura de telecomunicacions, el tall de trànsit als proveïdors de serveis d'internet (ISP, per les seves sigles en anglès) i el bloqueig de l'accés al combustible necessari per alimentar els serveis de

336 **Amnistia Internacional.** "Devices of Palestinian HHRR defenders hacked". 8 de novembre del 2021. Disponible a: https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

337 **Adalah.** "Adalah monitorea las violencias de la guerra". 27 d'octubre del 2023. Disponible a: https://www.adalah.org/ar/content/view/10939

338 **7amleh.** "Briefing on the Palestinian Digital Rights Situation since October 7th 2023". 2023. Disponible a: https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

339 Defensora de drets humans palestina, entrevista realitzada en el marc de The Nonviolence Factory, novembre del 2023. Equipo NOVACT, SUDS, IRIDIA y ODHE.

telecomunicacions.[340] En conjunt, aquests tancaments han mantingut la població de Gaza desconnectada gairebé del tot i greument aïllada.[341]

Des del 7 d'octubre del 2023, les defensores de drets humans, influencers i blogueres palestines s'han enfrontat a més censura en línia. Aquesta censura ha estat particularment forta a les plataformes propietat de Meta:[342] Facebook i Instagram,[343] tot i que també en altres plataformes com X[344] (antiga Twitter) o Telegram, on les defensores de drets humans han documentat el silenciament sistemàtic de les veus palestines, a través de l'eliminació arbitrària de continguts,[345] la suspensió de comptes palestins i les restriccions a usuaris i continguts propalestins.

"Des de l'inici del genocidi, les autoritats israelianes han utilitzat les apagades d'internet com a eines de càstig col·lectiu, a través d'una sèrie de tàctiques, com ara la imposició d'apagades intermitents de les comunicacions que coincideixen amb intensos bombardejos, la destrucció de la infraestructura de telecomunicacions, el tall de trànsit als proveïdors de serveis d'internet (ISP, per les seves sigles en anglès) i el bloqueig de l'accés al combustible necessari per alimentar els serveis de telecomunicacions"

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

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

342 A**ccess Now.** "How Meta censors Palestinian voices". 2024.
Disponible a: https://www.accessnow.org/publication/how-meta-censors-palestinian-voices

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

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

345 **7Amleh.** "Briefing on the Palestinian Digital Rights Situation". 2024.
Disponible a:
https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

VIII

JORDÀNIA: LA DERIVA A L'AUTOCENSURA

El panorama polític de Jordània, considerat un "Cavall de Troia" al Mashreq,[346] ha experimentat una important transformació en l'última dècada. Aquest canvi ha estat influït especialment per la Primavera Àrab, la pandèmia de la COVID-19 i diversos esdeveniments sociopolítics posteriors. Un element central d'aquests canvis ha estat la creixent dependència del Govern jordà de la vigilància massiva com a eina per mantenir el control polític i l'ordre públic.

L'entorn polític de Jordània s'ha caracteritzat per una barreja de monarquia tradicional i estructures estatals modernes, amb el rei Abdalá II al capdavant. La Primavera Àrab va portar a Jordània onades de protestes antigovernamentals[347] que, al principi, la monarquia va adreçar amb promeses de reforma i més llibertats. Tanmateix, aquestes promeses aviat van ser eclipsades per mesures estrictes, destinades a frenar la dissidència. L'any 2013, per exemple, el Govern de Jordània va bloquejar 304 llocs web de notícies, en virtut d'una controvertida llei de publicació, mesura que es va considerar un atac directe a la llibertat de premsa.[348]

La Direcció General d'Intel·ligència (GID), també coneguda com a "*mukhabarat*", ha tingut un paper cabdal en aquestes activitats de vigilància que fa ús de tecnologies avançades.[349]

La introducció de la Llei de la ciberdelinqüència, l'any 2015 va marcar un important punt d'inflexió en els esforços del Govern per controlar les comunicacions digitals.[350] Aquesta llei, que inclou càrrecs com "difondre notícies falses" i "incitar a la violència" s'ha fet servir sovint per processar periodistes i defensores de drets humans. Aquesta eina legal ha permès al Govern exercir més control sobre les activitats en línia, allò que ha provocat un augment de la censura i l'autocensura entre aquelles persones que s'atreveixen a alçar la veu.[351]

346 La noció de "cavall de Troia" suggereix que Jordània podria estar tenint un paper ocult o estratègic, en benefici d'interessos externs o diferents d'aquells que aparenta, en una regió caracteritzada per tensions polítiques. Això implica que Jordània podria estar facilitant l'entrada o la influència de potències externes a l'Orient Mitjà de manera discreta.

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

348 **Jamal Halaby.** "Jordan: 304 national news website blocked". AP News. 3 de juny del 2013.
Disponible a: https://apnews.com/article/b1b0f9f29a5d4368b7a97792b76570ce

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

350 **Dentons.** "Cybercrime Law in Jordan". 16 d'octubre del 2023.
Disponible a: https://www.dentons.com/en/insights/alerts/2023/october/16/cybercrime-law-in-jordan

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

1. BLOQUEIG D'INTERNET PER SILENCIAR VEUS DISSIDENTS I NEUTRALITZAR LA MOBILITZACIÓ SOCIAL.

Els darrers anys, el Govern jordà ha actuat de manera contundent per tancar llocs web de notícies independents, una clara demostració de la seva estratègia amb el control del flux d'informació i la repressió de les dissidències. Aquesta acció s'executa principalment, en virtut de la controvertida Llei de premsa i publicacions del 2013,[352] l'objectiu aparent de la qual és impedir la difusió d'informació falsa i mantenir la seguretat nacional. No obstant això, a la pràctica, aquesta llei s'ha utilitzat per suprimir qualsevol forma de mitjà de comunicació que no s'alineï amb la narrativa del Govern, fet que soscava significativament la llibertat de premsa del país. La persecució col·lectiva dels mitjans de comunicació independents ha tingut un profund impacte en el panorama dels mitjans de comunicació a Jordània.

La nova Llei de Ciberdelinqüència, a través del seu article 37, permet al Govern tancar i bloquejar pàgines web i aplicacions que la incompleixen.[353] Plataformes com TikTok, Clubhouse, Facebook live, Al-Hudood o 7iber han estat bloquejades temporalment. Segons fons governamentals, aquestes plataformes i aplicacions van ser bloquejades per presumptament difondre desinformació o incitar a la violència.[354] No obstant això, les plataformes van ser bloquejades durant les mobilitzacions massives al país, com la vaga de professores del 2020 o la de camioneres a la ciutat de Maan, l'any 2022, per evitar que les defensores de drets humans poguessin difondre'n imatges i notícies.[355] A més, Jordània és un dels països de la regió que més demandes d'informació realitza a les grans empreses de xarxes socials. Agències com la Comissió de Mitjans Jordans, la Comissió Reguladora de Telecomunicacions o altres agències de seguretat tenen competències per tancar o suspendre temporalment aquestes pàgines web.

Aquesta censura digital es du a terme a través de diferents estratègies que inclouen l'ús de tecnologies avançades de control d'internet. La tecnologia utilitzada per aplicar aquestes

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

353 **Salam Freihat.** "Jordan's Cybercrime Law to Limit Investments and E-commerce," SMEX. 30 d'agost del 2023. Disponible a: https://smex.org/jordans-cybercrime-law-to-limit-investments-and-e-commerce/

354 **Abdullah Jbour.** "Jeopardizing Digital Rights in Jordan" Carnegie Endowment for International Peace. 15 d'agost del 2023. Disponible a: https://carnegieendowment.org/sada/2023/08/jeopardizing-digital-rights-in-jordan?lang=en

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

mesures inclou sofisticats sistemes de filtratge d'internet com la DPI,[356] que bloquegen URLs i bloquegen continguts específics, a partir de paraules clau i altres indicadors.[357] Una empresa estatunidenca ha desenvolupat i posat en funcionament el programa Smart Filter a Jordània,[358] que permet al Govern filtrar i bloquejar continguts en línia, considerats inapropiats o una amenaça per a la seguretat nacional. Aquest programa s'ha utilitzat per censurar continguts en línia i restringir l'accés a la informació, alhora que coarten la llibertat d'expressió.[359] L'ús d'aquest programa s'ha intensificat notablement després de la COVID-19. A més, les empreses proveïdores de serveis d'internet també estan obligades a complir les directives governamentals per bloquejar l'accés a determinats llocs web i vigilar les activitats en línia de les usuàries, mentre s'assegura l'aplicació exhaustiva d'aquestes mesures de censura.[360]

2. PIRATEIG MASSIU DEL PERIODISME INDEPENDENT

La persecució de periodistes i professionals que intenten treballar al marge de l'estricta normativa del Govern és també una pràctica habitual a Jordània. La Llei de ciberdelinqüència, la Llei de Telecomunicacions i la Llei de prevenció de delictes són les eines principals utilitzades per criminalitzar aquestes professionals, ja que possibiliten eludir els procediments judicials habituals i permeten a les forces de seguretat de l'Estat poder detenir persones, sense supervisió judicial.[361] La Llei de ciberdelinqüència i en concret els articles 15 i 17 ha estat una eina clau per criminalitzar periodistes i personal dels mitjans de comunicació, alhora que atorga al Govern amplis poders discrecionals per suprimir la llibertat de premsa.

Entre els casos més rellevants, destaca l'empresonament de la periodista Hiba Abu Taha, per una denúncia presentada per la Comissió de Mitjans de Comunicació, el 13 de maig del 2024, en relació amb els articles 15 i 17 de la Llei de ciberdelinqüència. Inicialment, el presumpte ciberdelicte es basava en la publicació d'un informe d'investigació al mitjà Annasher, on es descrivien les relacions de complicitat entre els Governs jordà i israelià

356 Vegeu glossari

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

358 Ibid. p. 9

359 Ibid

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

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

en relació amb el genocidi de Gaza, a través de l'establiment d'un corredor terrestre entre tots dos països per subministrar materials a Israel.[362] Tanmateix, posteriorment es va descobrir que l'acusació se centrava en un article on Taha criticava el Govern jordà per permetre a Israel utilitzar l'espai aeri jordà per interceptar míssils d'Iran.[363] Tot i els esforços per aconseguir el seu alliberament, Hiba segueix empresonada a la presó de Juwaida.[364] Un altre cas similar és el d'una estudiant de periodisme que s'enfronta a una deportació imminent a Síria, tot i estar registrada com a sol·licitant d'asil a l'ACNUR, des del 2013. La seva detenció, el 9 d'abril del 2024, mentre filmava una manifestació i el posterior empresonament, sense procediment judicial, posen de manifest l'ús de la Llei de Prevenció de Delictes per eludir els processos legals habituals.[365] El cas d'Abdul Jabbar Zeitoun mostra la discrecionalitat de les forces de seguretat de l'Estat. Zeitoun, fotoperiodista independent, va ser detingut i retingut durant una setmana, al març del 2024, mentre cobria unes protestes en contra de la guerra, tot i haver-se identificat immediatament com a periodista, en el moment de la seva detenció.[366]

Les dones periodistes són especialment vulnerables i s'enfronten a l'assetjament, la intimidació i la persecució. Una persona va ser multada amb 5000 dinars, en virtut de la Llei de ciberdelinqüència per difondre suposadament notícies falses i difamar institucions oficials. Detinguda inicialment el desembre del 2023, va ser alliberada més tard i la multa finalment es va anul·lar, en virtut d'una llei d'amnistia.[367] La persecució personal i col·lectiva de periodistes i mitjans de comunicació ha creat un clima de por i repressió, on els riscos de denunciar són elevats i les vies per fer-hi són cada vegada més limitades. Segons l'expert en comunicació Mohammed Shamma, "a causa d'aquest clima de repressió, la gent del meu voltant té por i per evitar qualsevol atac, s'autocensuren i redueixen el seu activisme i la seva activitat a les xarxes socials".[368]

"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"

362 **Committee to protect journalists.** "Palestinian-Jordanian Journalist Hiba Abu Taha Sentenced to One Year in Prison." 6 de juny del 2024.
Disponible a:
https://cpj.org/2024/06/palestinian-jordanian-journalist-hiba-abu-taha-sentenced-to-one-year-in-prison

363 **Hiba Abu Tahar.** "رود الرأي في الدفاع عن كيان العدو," Annasher. 22 d'abril del 2024.
Disponible a: https://annasher.com/exclusive/12857/

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

365 Ibid.

366 Ibid.

367 Ibid.

368 Mohammed Shamma, entrevista personal realitzada per l'equip d'investigació, 25 de juny del 2024.

La tecnologia de l'empresa israeliana NSO Group ha estat essencial per reprimir el periodisme independent a Jordània. Segons un informe d'Acces Now, entre el 2019 i el 2023, 35 defensores de drets humans i líders polítiques de les quals, 16 eren periodistes, van ser atacades amb el programari espia[369] Pegasus, de NSO Group.[370] Entre les periodistes afectades, destaquen dues periodistes del projecte *Organized Crime and Corruption Reporting Project*, el fotoperiodista i documentalista independent Abdul Jabbar Zeitoun, que va ser detingut el 21 de març del 2024 durant unes protestes contra la guerra o la ja esmentada periodista Hiba Abu Taha. Segons Mohammed Shamma, "l'objectiu és silenciar veus i reprimir defensores de drets humans i periodistes, a través de lleis i tecnologies que es van fer servir durant el període del Coronavirus".[371] Pegasus va seguir sent un component fonamental de l'estratègia de vigilància de Jordània, després de la COVID-19.

3. VIOLÈNCIA DIGITAL CONTRA DEFENSORES DELS DRETS HUMANS I PERSONES LGBTIQ+

L'entorn sociopolític de Jordània ha vist com augmentava la repressió contra les defensores de drets humans, caracteritzada per detencions, intimidacions i vigilància, a l'empara d'amplis marcs legals com el Codi Penal i la Llei de ciberdelinqüència i la Llei antiterrorista del 2006.[372] La comunitat LGBTIQ+ es troba entre els col·lectius més afectats pe control i la repressió institucional. Al panorama jordà s'han produït cada vegada més detencions i intimidacions de persones LGBTIQ+, també en virtut del Codi Penal i la Llei antiterrorista, especialment. Alguns casos notables són la detenció del director d'un centre LGBTIQ+, detingut per la policia, i la detenció de defensores de drets humans, acusades de posar en perill la seguretat nacional.[373] L'experta en comunicació Yara Harare assegura que el Govern ataca drets civils i polítics per anul·lar l'espai cívic i atacar qualsevol grup que intenti

369 Vegeu glossari

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

371 Mohammed Shamma, entrevista personal realitzada per l'equip d'investigació, 25 de juny del 2024.

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

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

transformar la societat jordana. En aquest sentit, Harare afegeix que la comunitat LGBTIQ+ està sent especialment reprimida, fet que provoca por i autocensura entre les seves activistes, fins a l'extrem de no poder dir públicament paraules com LGBTIQ+ o queer.[374]

La infraestructura tecnològica forma part d'una estratègia més àmplia de vigilància i control de les comunicacions digitals, que inclou la vigilància de les usuàries dels cibercafès i el registre obligatori de les targetes SIM. En aquest sentit, es van introduir normatives que obliguen els cibercafès a mantenir registres detallats de les identitats de les usuàries, vigilar les activitats mitjançant càmeres de seguretat i registrar els llocs web visitats.[375] A més, el registre obligatori de les targetes SIM amb les dades del document nacional d'identitat o el passaport, incloses les dades biomètriques, ha facilitat una àmplia vigilància de les telecomunicacions.[376] Aquest requisit ha permès a les autoritats el rastreig i la intercepció de les comunicacions, fet que coartava encara més l'anonimat i la llibertat d'expressió.

Aquest sistema de vigilància massiva té un impacte directe en la llibertat d'expressió i l'espai cívic a Jordània. Destacades defensores de drets humans, com l'advocat Malik Abu Orabi, van ser objecte de nombrosos atacs amb el programa espia Pegasus entre agost del 2019 i juliol del 2021.[377] Ahmad Al-Neimat, defensor dels drets humans i activista contra la corrupció, va patir el pirateig del seu telèfon el gener del 2021 i es va enfrontar a diverses detencions.[378] A Lama Fakih, directora per l'Orient Mitjà i el Nord de l'Àfrica de Human Rights Watch, li van infectar el seu iPhone cinc vegades amb el programa espia Pegasus entre l'abril i l'agost del 2021 i Hiba Zayadin, investigadora principal de Human Rights Watch va rebre múltiples notificacions d'Apple l'any 2023 on l'informaven que el seu telèfon estava essent atacat per programaris espia[379] patrocinats per agents governamentals.[380]

374 Yara Harare, entrevista personal realizada por el equipo de investigación, 14 de juny del 2024.

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

376 Ibid.

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

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

379 Vegeu glossari

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

Aquest entorn repressor fomenta l'autocensura i la por entre periodistes, defensores de drets humans i persones LGBTIQ+ i soscava les llibertats civils i els valors democràtics a Jordània. Segons Yara Harare, Jordània[381] és líder en encobriment de casos de persecució d'activistes: "Hi ha una apagada informativa sobre aquests casos a escala internacional".[382]

"Jordània és líder en encobriment de casos de persecució d'activistes: "Hi ha una apagada informativa sobre aquests casos a escala internacional"

4. VIGILÀNCIA I REPRESSIÓ DE LES PROTESTES CONTRA EL GENOCIDI A GAZA

La censura de la informació militar i de seguretat a Jordània s'ha intensificat significativament des de l'octubre de 2023, fet que posa de manifest els esforços continuats del Govern per controlar la informació i suprimir qualsevol forma de dissidència, en relació amb les operacions de seguretat i les implicacions que tenen en l'actual conflicte de Gaza. Les principals eines jurídiques que faciliten aquesta censura i repressió són la Llei de ciberdelinqüència, en concret els articles 15 i 17 i la Llei de prevenció de delictes.

Els atacs indiscriminats d'Israel contra la població de Gaza van provocar una gran indignació a Jordània que va desembocar en manifestacions multitudinàries espontànies davant l'ambaixada d'Israel, al districte de Rabyeh, a Amman. Durant el 2024, Mohammed Shamma ha documentat 11 casos d'obstrucció de l'activitat de periodistes, en alguns casos, fins i tot amb detencions, per cobrir les manifestacions pro-palestines.[383] Alguns casos rellevants són Khair Al Jabri, que va ser detingut el març del 2024, en virtut de la Llei de ciberdelinqüència, per tornar a publicar un videoclip que criticava l'actuació de les forces policials a les protestes per Gaza.[384] Un fotoperiodista va ser detingut, el març del 2024, mentre cobria les protestes a la zona de Rabyeh i retingut gairebé un mes. Tot i la decisió del fiscal d'alliberar-lo, el governador va insistir a empresonar-lo, fet que indica

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

382 Yara Harare, entrevista personal realizada por el equipo de investigación, 14 de juny del 2024.

383 Mohammed Shamma, entrevista personal realitzada per l'equip d'investigació, 25 de juny del 2024.

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

una actitud punitiva cap a la informació sobre successos relacionats amb la seguretat.[385] Per últim, una realitzadora audiovisual va ser pressionada per la GID el març del 2024 perquè signés un compromís de no participar en protestes com les pro-palestines que suposen una amenaça per la seguretat del país. Aquests casos posen en relleu una pauta d'utilització de marcs jurídics, com ara la Llei de ciberdelinqüència i la Llei de prevenció de delictes per reprimir les dissidències i vigilar la societat civil.[386]

Per obstruir i perseguir l'activitat periodística, es fa servir un exhaustiu monitoreig de les xarxes socials per identificar continguts digitals i controlar i fer seguiment de les manifestacions. La Comissió de Mitjans de Comunicació i la GID són agències rellevants en aquesta vigilància massiva. Tanmateix, es desconeix qui està gestionant la captura d'imatges a través de càmeres de videovigilància que han estat col·locades de manera estratègica a la zona de protesta, a Rabyeh. Segons indica una investigadora de la Jordan Open Source Association, aquestes càmeres són diferents de les càmeres de control del trànsit que es poden trobar a la ciutat d'Amman i que capturen imatges gestionades pel Centre de Control del Trànsit, sota el control de la Direcció de Seguretat Pública i Protecció civil.[387]

385 Ibid.

386 Ibid.

387 **Yara AlRafie**, "Public Cameras/CCTV Amman", Jordan Open Source Association. 21 d'agost del 2022. Disponible a: https://www.josa.ngo/blog/217

IX

L'IRAQ: LA MILITARITZACIÓ DE L'ESPAI DIGITAL

L'octubre del 2019, milers de manifestants van sortir als carrers de Bagdad i d'altres ciutats del sud del país, en contra de la corrupció del Govern. Tot i el caràcter no violent del moviment social Thishreen,[388] les forces de seguretat de l'Iraq i milícies vinculades al Govern van assassinar prop de 500 persones, durant els primers 7 mesos de la revolta popular.[389] La repressió es va traslladar també als espais digitals, on les publicacions de suport a les mobilitzacions van comportar detencions fulminants per part d'agents d'unitats antiterroristes.[390] Des del 2003, l'Iraq ha anat derivant en un dels governs més restrictius de la regió Mashreq, amb un marc legal que ataca les llibertats civils de la societat.

La persecució de la dissidència política a l'Iraq ha estat una pràctica comuna, des de l'inici del període colonial britànic i el règim de Saddam Hussein. Amb la caiguda del dictador, es va produir una obertura de l'espai cívic, amb milers d'organitzacions no governamentals i mitjans de comunicació registrats al país. Entre el 2003 i el 2019, es van crear més de 200 noves estacions de ràdio a l'Iraq.[391] Paral·lelament, els serveis d'intel·ligència iraquians també es van modernitzar, amb l'ajuda dels Estats Units d'Amèrica i el Regne Unit, per lluitar contra la insurgència al país.[392] A partir de la derrota del Daesh (Estat Islàmic de l'Iraq i Síria), el 2017, les tecnologies de vigilància van passar a utilitzar-se en altres esferes de la seguretat nacional per defensar els valors de la nació. A la pràctica, això es va traduir en un augment de la vigilància massiva de defensores de drets humans i periodistes, al país.[393] Es calcula que 1,3 milions de persones a l'Iraq estan en risc de patir violència digital, el 75 % de les quals són dones i nenes.[394]

---

388 Moviment Thishreen és com s'ha denominat el moviment social sorgit durant les protestes a l'Iraq entre el 2019 i el 2021. El principal centre de les protestes va ser la plaça Tahrir de Bagdad, juntament amb altres protestes que es van produir a Bàssora i Najaf.

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

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

391 **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 a:
https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

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

393 **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 a:
https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

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

1. PRÀCTIQUES ANTITERRORISTES PER A NEUTRALITZAR LA DISSIDÈNCIA POLÍTICA IRAQUIANA

L'arquitectura de la seguretat nacional a l'Iraq té un caràcter predominantment militar, a causa de dècades de lluita contra el terrorisme. El 2009, el primer ministre iraquià Nour Al-Maliki, amb el suport de les agències d'intel·ligència de la CIA, l'MI6 britànic i la Falcon Cell, una unitat d'intel·ligència especialitzada en la lluita contra el terrorisme i amb poders per investigar i neutralitzar amenaces de seguretat nacional, sense necessitat d'ordres judicials. D'altra banda, el Govern nord-americà va transferir tecnologia per a monitorar i enregistrar trucades telefòniques i missatges de text telefònics amb l'objectiu de prevenir atacs terroristes.[395] Una d'aquestes eines d'espionatge podria ser la tecnologia Stingray: antenes simuladores de telecomunicacions que permeten interceptar comunicacions mòbils i generar sistemes de monitoratge de trucades i SMS.[396] A mitjan 2023, el nou primer ministre, Mohammed Shia Al-Sudani, va nomenar Abu Ali al-Basri, fins llavors cap de la Falcon Cell, com a responsable dels Serveis de Seguretat Nacional Iraquiana (INSS, pel seu acrònim en anglès).[397]

El control dels serveis d'intel·ligència per part de militars[398] i l'aplicació de lleis i pràctiques antiterroristes, han contribuït a representar a la dissidència política com una amenaça per a la seguretat nacional. La Llei antiterrorista núm.13 del 2005 inclou ambigüitats en la seva definició" d'acte terrorista" entès com a qualsevol amenaça que atempti contra

395 **Radio Free Europe.** "U.S. Providing Irak with Phone, SMS Monitoring Devices" Radio Free Europe/Radio Liberty. 21 d'agost del 2011.
Disponible a:
https://www.rferl.org/a/us_providing_Irak_with_phone_and_sms_monitoring_devices/24303623.html

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

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

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

la "unitat nacional".[399] El Govern va fer servir la llei antiterrorista per vigilar i detenir defensores de drets humans de les mobilitzacions d'octubre del 2019 i ho va justificar assegurant que les protestes eren violentes i alteraven l'ordre social del país. Per exemple, a la regió d'Anbar, algunes joves van ser arrestades pels serveis antiterroristes poc després de fer publicacions a Facebook, en les quals mostraven el seu suport al moviment Thishreen, l'any 2019.[400]

Els serveis de seguretat nacional iraquians poden obtenir dades personals i continguts de trucades, missatges i correus electrònics, a través de les principals empreses de telecomunicacions del país, en casos de seguretat nacional. Es calcula que vora de 40 milions d'iraquians tenen subscripcions de telefonia mòbil i 20 milions tenen subscripcions d'internet amb les dues principals empreses del país, Zain Irak i Asian Cell. Aquestes empreses estan obligades a donar les dades personals, com la localització, missatge i altres tipus de comunicacions dels seus usuaris, si hi ha una autorització judicial. La interacció d'aquestes empreses amb la INSS per a casos de seguretat nacional és molt freqüent.[401]

En aquest sentit, un informe del 2020 de la Peace and Freedom Organization descriu l'augment de la vigilància massiva en períodes electorals.[402] L'objectiu de la vigilància és persuadir i neutralitzar les veus dissidents, a través de diferents estratègies com l'extorsió digital[403] o la violència física. Durant els mesos previs a les eleccions parlamentàries del 2021, diverses defensores de drets humans van ser assassinades i més de 30 periodistes van ser arrestats a la província de Dhi-Qar.[404] La persecució i repressió de defensores de drets humans de la ciutat de Nassiriyah, a Dhi Qar tenia l'objectiu concret de controlar i intimidar dues formacions polítiques oposades al Govern, com Imtidad i Al-Bait al-Watani.[405] La persecució de la dissidència política continua en l'actualitat també a la Regió del Kurdistan Iraquià (KRIm pel seu acrònim en anglès, amb alguns casos molt recents com la detenció de Shakar Star del mitjà Tiwar News per part de l'agència d'intel·ligència kurda

399 **Official Gazette of Iraq.** "Anti-Terrorism Law No."Anti-Terrorism Law No. (13) of 2005". Disponible a: 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

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

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

402 **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 a: https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

403 Vegeu glossari

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

405 Ibid

Asayish, per presumiblement preparar i publicar un informe que s'argumentava que incitava a la violència i la desinformació.[406]

La repressió també ha comportat assassinats de defensores de drets humans[407] darrere dels quals hi hauria milícies armades, vinculades amb partits polítics de l'Iraq i el Govern de l'Iran. Entre aquestes milícies, destaquen les Forces de Mobilització Popular (PMF, pel seu acrònim en anglès),milícies predominantment xiïtes que van ser creades per defensar les comunitats locals de l'amenaça del Daesh. Tanmateix, actualment, les PMF són responsables d'atacs sistemàtics contra defensores de drets humans i comunitats vulnerabilitzades.[408] Tot i que el Govern iraquià ha intentat integrar-les a les forces i cossos de seguretat de l'Estat, segueixen operant al marge de la llei. Per exemple, l'any 2020, Hisham al-Hashim, analista especialitzat en jihadisme, va ser assassinat per un militant de la milícia pro-iraniana Kataeb Hezbollah, per les seves crítiques al Govern i als grups armats no estatals.[409]

2. APAGADES DIGITALS PER A DESARTICULAR LES MOBILITZACIONS SOCIALS I SILENCIAR LA VIOLÈNCIA INSTITUCIONAL

L'Iraq és un dels països del món que més utilitza la interrupció de l'accés a internet com a estratègia per silenciar l'activisme polític.[410] Des del 2029, el Govern va bloquejar l'accés a

406 **Committee to protect journalists.** "Iraqi Kurdish Asayish Security Forces Arrest Journalist Shakar Star After Smuggling Reports". 21 de maig del 2024.
Disponible a:
https://cpj.org/2024/05/iraqi-kurdish-asayish-security-forces-arrest-journalist-shakar-star-after-smuggling-reports/

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

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

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

410 **Access Now.** "Shrinking democracy, growing violence. Internet Shutdowns in 2023,". Maig del 2024.
Disponible a: https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

"Durant els períodes de bloqueig d'internet, la violència de la policia i de les milícies contra les defensores de drets humans augmenta, perquè no es poden difondre immediatament les imatges i vídeos d'aquests atacs."

internet en 126 ocasions.[411] Moltes d'aquestes apagades digitals es van produir durant les protestes socials. Per exemple, durant les manifestacions del moviment Thishreen, l'octubre del 2019, el Govern va bloquejar l'accés a internet durant més de 50 dies. Durant aquest període, 23 civils van ser assassinats, a mans de les forces de seguretat de l'Estat i grups paramilitars com PMF.[412] Segons Hayder Hamzoz, director del la INSM Foundation for Digital Rights, durant els períodes de bloqueig d'internet, la violència de la policia i de les milícies contra les defensores de drets humans augmenta, perquè no es poden difondre immediatament les imatges i vídeos d'aquests atacs.[413] També va haver-hi apagades digitals durant el terratrèmol que va afectar Síria i el nord de l'Iraq, fe que va provocar un impacte negatiu en la distribució de l'ajuda humanitària.[414] Diverses organitzacions internacionals i locals han iniciat diverses campanyes contra aquestes pràctiques, entre les quals destaca #KeepItOn.[415]

Els bloquejos d'internet van ser utilitzats per primera vegada l'any 2014 per les autoritats iraquianes per lluitar contra el terrorisme de l'Estat Islàmic. Des d'aleshores, tal com apunta l'expert en drets humans Ismaeel Dawood, el Govern ha anat sofisticant aquesta estratègia i incloent la coordinació amb les autoritats de la Regió del Kurdistan Iraquià (KRI) i les empreses proveïdores de serveis de telecomunicacions i aplicacions del país.[416]

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

412 **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 desembre del 2020.
Disponible a:
https://timep.org/2020/12/17/from-free-space-to-a-tool-of-oppression-what-happened-to-the-internet-since-the-arab-spring/

413 Hayder Hamzoz, entrevista personal realitzada per l'equip de recerca, 4 de juny del 2024.

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

415 **Access Now.** "Keep It On." Disponible a: https://www.accessnow.org/campaign/keepiton/

416 Ismaeel Dawood, entrevista personal realitzada per l'equip d'investigació, 20 de juny del 2024.

3. EL CONTROL DELS CONTINGUTS DIGITALS: CENSURA I VIGILÀNCIA MASSIVA

El marc normatiu que regula els ciberdelictes no només és obsolet, sinó que s'utilitza per limitar la llibertat d'expressió i el dret a la no discriminació. Els delictes als espais digitals es regulen per la Llei Civil núm. 49 de 1951, la Llei de comunicacions del 2004 i el Codi Penal núm. 11 de 1969.[417] Per exemple, el Codi Penal iraquià, que conté provisions que s'utilitzaven durant l'ocupació britànica, criminalitza continguts digitals que suposin una "indecència pública" (art. 401 i 403)[418] o que pretenguin "canviar els principis fonamentals de la Constitució o les lleis bàsiques de la societat".[419] Així mateix, el Govern del KRI disposa de la "Llei per prevenir l'ús indegut de les telecomunicacions" per sancionar inclús amb penes de presó, la difusió d'amenaces, la difamació, la desinformació i les injúries, entre d'altres, que atemptin contra l'honor o incitin a cometre un delicte moral.[420] L'any 2021, membres de l'organització kurda pro-drets LGBTIQ+ Rasan, van ser arrestades per la policia per la difusió de contingut digital "contrari a la moral de la nació". Les autoritats van apel·lar a l'article 401 del Codi Penal.[421] La repressió contra Rasan va culminar el maig del 2023, quan un tribunal del KRI va ordenar el tancament de l'organització.[422]

Existeixen dos mecanismes governamentals per implementar aquest marc legal. Per una banda, la Comissió de Comunicacions i Mitjans (CMC, pel seu acrònim en anglès) creada el 2004, que du a terme la vigilància massiva i el control dels continguts digitals de la societat civil, interactuant amb les grans empreses de telecomunicacions de l'Iraq.[423] Paral·lelament, des del 2009, el Ministeri de Comunicacions ha signat diversos contractes amb

417 **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 a:
https://www.researchgate.net/publication/360024571_Invisible_Threats_Digital_Security_and_Female_Journalists_in_Iraq_and_the_Kurdistan_Region

418 L'article 401 del Codi Penal castiga tota persona que cometi un "acte indecent" amb penes de fins a sis mesos de presó o multa o totes dues penes. L'articla 403 del Codi estipula que tota persona que produeixi o publiqui materials que atemptin contra la moral pública o la decència, amb la intenció d'explotar o distribuir aquests materials serà castigada amb penes de presó de fins a dos anys o multa o totes dues penes.

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

420 Ibid

421 Ibid

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

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

empreses franceses, probablement Safran i Thales,[424] perquè subministrin un sistema de monitoreig d'internet i de bloqueig de pàgines web.[425] En el mateix període, el centre d'investigació Citizen Lab va identificar aplicacions de l'empresa Blue Coat Systems que permeten la vigilància massiva, a les xarxes de telecomunicacions de Bagdad vinculades a la xarxa City Telecom.[426]

D'altra banda, al gener del 2023, el Ministeri de l'Interior va crear el Comité de Monitoreig de Contingut Digital per vigilar i censurar els continguts digitals que són nocius o contraris a les normes socials i culturals del país.[427] A aquest efecte, el comitè va llançar aquell mateix any la plataforma "Balgh" ("Informa) perquè la societat civil denunciï "continguts de xarxes que atemptin contra la moral pública, continguin missatges negatius indecents i soscavin l'estabilitat social", segons paraules del Ministre de l'Interior.[428] En només un més, es van rebre 96 000 denúncies de la societat civil,[429] algunes de les quals van seguir en processos legals, d'acord amb l'article 403 del Codi Penal. Segons Amnistia Internacional, aquest mateix any el comitè va traslladar 16 casos als tribunals penals[430] Algunes figures públiques, models i artistes com Assal Houssam, Hassan Sajmah, Sayyed Ali, Saealusa i Umm Fahd han estat arrestades o sancionades per la publicació de contingut "indecent", arran d'aquests nous mecanismes.[431] Com a mínim 6 d'elles han estat sentenciades a penes de presó el 2023[432] i com a mínim una ha estat assassinada.[433]

---

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

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

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

427 **Iraki News Agency.** Ministeri de l'Interior: formar un comitè per monitorar el contingut als llocs de les xarxes socials i responsabilitzar-ne els creadors. 16 de gener del 2023.
Disponible a:
https://www.ina.iq/175883--.html?__cf_chl_tk=wVv0deBsEkhWjoMlC5MepZzKdePd.PmTxkLzbeEojyg-1719559517-0.0.1.1-4543

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

429 Hayder Hamzoz, entrevista personal realitzada per l'equip de recerca, 4 de juny del 2024.

430 **Amnistia Internacional.** "Iraq: Government must match rhetoric on human rights with meaningful action." 15 de març del 2023.
Disponible a:
https://www.amnesty.org/en/latest/news/2023/03/iraq-government-must-match-rhetoric-on-human-rights-with-meaningful-action/

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

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

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

Les propostes de llei actuals per regular els espais digitals apunten inclús a més restriccions de la llibertat d'expressió a l'Iraq. En l'actualitat, el Govern de l'Iraq debat un esborrany de Llei de ciberdelinqüència que inclou penes de presó de fins a 10 anys, per publicar continguts digitals que atemptin contra els principis religiosos i socials del país.[434] La Comissió de Comunicacions i Mitjans (CMC) també està desenvolupant la Regulació núm. 1 de 2023 sobre contingut digital per suprimir el contingut en línia i sancionar delictes de les usuàries d'internet.[435] Paral·lelament, es debaten la Llei d'accés a la informació i la Llei de llibertat d'expressió, que totes dues inclouen ambigüitats legals que es podrien utilitzar per restringir llibertats civils.[436] Finalment, l'esborrany de la Llei de reorganització dels mitjans electrònics també ha aixecat moltes crítiques, especialment per l'impacte negatiu que pot tenir sobre la llibertat d'expressió i la llibertat de premsa.[437]

4. CAMPANYES D'ASSETJAMENT I INCITACIÓ A L'ODI CONTRA COL·LECTIUS VULNERABILTZATS

Les campanyes d'incitació a l'odi en les esferes digitals també són una constant a l'Iraq. Alguns líders polítics, religiosos i militars promouen el discurs de l'odi per exacerbar les divisions sectàries i guanyar influència política. L'any 2022, un clergue i líder xiïta va demanar a la societat iraquiana, a través d'una publicació a la plataforma X (abans Twitter) lluitar contra la comunitat LGBTIQ+, un acte que va contribuir a la intensificació del discurs de l'odi a les xarxes socials.[438] En aquesta línia, el grup de drets humans Iraqi Media House assegura que el "fenomen dels exèrcits electrònics ha assolit nivells perillosos per

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

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

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

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

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

l'emissió d'amenaces, inclosa la incitació a la violència i l'odi".[439] Així mateix, alguns casos demostren que algunes dones candidates polítiques han estat objecte[440] d'extorsions digitals,[441] campanyes d'incitació a l'odi i amenaces, amb l'objectiu que abandonessin les seves carreres polítiques.[442] Paral·lelament, Nacions Unides assegura que, des del 2016, com a mínim 36 defensores de drets humans han estat assassinades, després d'haver estat acusades de ser agents estrangers o terroristes, per comptes no autentificades, bots i canals de Telegram.[443]

Les campanyes d'assetjament en línia combinen pràctiques de dòxing,[444] publicació de dades personals i notícies falses[445] que posen seriosament en perill les persones. Les dones es veuen especialment afectades per la violència digital.[446] Segons la Missió de les Nacions Unides per l'Iraq (UNAMI), hi ha campanyes anònimes que exposen públicament dones i nenes que han participat en manifestacions en contra del Govern, amb denúncies per "conductes immorals", a través d'imatges manipulades.[447] Durant les manifestacions de l'octubre del 2019, aquesta violència digital va fer que moltes dones deixessin de participar a les manifestacions. Un cas especialment rellevant va ser l'assassinat, el 2020, de l'activista Reham Yacoub, després d'una campanya de desinformació on l'acusaven de tenir vincles amb agents nord-americans.[448]

El col·lectiu LGBTIQ+ és especialment sensible a les campanyes d'assetjament en línia per part del Govern i les milícies. Segons Human Rights Watch, la vigilància, l'assetjament i les

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

440 **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 a: https://t4p.co/article/2021-07-21-the-journalist-nour-al-jawahiri

441 Vegeu glossari

442 **Orto, N.** Iraq elections: Why some female candidates refused to run. The New Arab. 8 d'octubre del 2021. Disponible a: https://www.newarab.com/features/iraq-elections-why-some-female-candidates-refused-run

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

444 Vegeu glossari

445 Vegeu glossari

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

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

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

amenaces en línia a persones LGBTIQ+ són una tendència creixent a la regió.[449] L'abril del 2024, el Govern Federal Iraquià va aprovar una llei que criminalitza i sanciona amb penes de presó de fins a 15 anys les relacions sexuals homosexuals. En aquest marc, es produeixen pràctiques d'entrampament[450] digital en aplicacions com Grindr, per forçar conductes de persones LGBTIQ+ que la llei qualifica d'immorals. A partir d'aquestes pràctiques, es produeixen arrestos arbitraris, tortura i altres tractes degradants i inhumans.[451] De la mateixa manera, les milícies també utilitzen les xarxes socials i aplicacions de cites en línia per extorsionar digitalment[452] [453] les persones LGBTIQ+.

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

450 Vegeu glossari

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

452 Vegeu glossari

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

CONCLUSIONS

En general, es visibilitza una tendència a l'autoritarisme i al control social a tota la regió, empès per l'aparició de noves eines tecnològiques, així com pràctiques d'infiltració en línia i suplantació d'identitat cada vegada més acomplexades i esteses. Una tendència que s'ha agreujat des de l'inici del genocidi a Gaza, l'octubre del 2023 que, sens dubte, deixa intuir una reblada més de clau en la repressió a les veus crítiques no només al Maghreb i el Mashreq, sinó també contra l'activisme dels països occidentals que denuncia la inacció de la comunitat internacional o expressa el seu suport al poble palestí.[1] [2]

En concret, s'identifiquen les tendències següents:

1. MARCS REGULADORS REPRESSIUS

El punt de partida de la vigilància massiva a les regions Maghreb i Mashreq són els entramats reguladors desenvolupats per controlar les dissidències polítiques. Els codis penals amb reminiscències dels períodes colonials es combinen amb noves lleis per controlar les formes emergents d'activisme i comunicació social, sota el pretext de la seguretat nacional i la defensa dels valors morals de l'Estat. En aquest sentit, observem d'una banda, l'ús de lleis i polítiques antiterroristes per retallar drets i ampliar els supòsits en què es permet la vigilància i la intercepció de comunicacions de la població. En tots els casos, el terrorisme ha estat un fantasma que s'ha aprofitat convenientment per presentar la dissidència política com una amenaça per la seguretat nacional. En casos com el de Tunísia, ha estat una excusa perfecta per limitar la mobilitat i la circulació interna i cap a l'estranger de persones migrants i de la dissidència política i de gènere.

Per altra banda, els règims autoritaris desenvolupen nous instruments legals per controlar els continguts i les noves formes d'organització digital. Les lleis contra la ciberdelinqüència que s'estan aprovant al Maghreb i al Mashreq es justifiquen per prevenir conductes "immorals", protegir la infància i prevenir la difusió de notícies falses, entre altres. No obstant això, la realitat és que han suposat un punt d'inflexió en el control de les comunicacions digitals, fet que ha revertit en un augment de la censura i l'autocensura entre aquells que s'atreveixin a alçar les seves veus crítiques, especialment, des d'àmbits com el periodisme independent, les organitzacions defensores de drets humans i el col·lectiu LGBTIQ+. Lluny d'evitar la circulació d'informació falsa, aquestes noves lleis estan essent

1 **Amnistia Internacional.** "Europe: Authorities must protect the rights to freedom of expression and peaceful assembly ahead of Nakba Remembrance Day". 10 de maig del 2024.
Disponible a:
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".
Recuperat de:
https://www.ohchr.org/es/documents/thematic-reports/a79319-global-threats-freedom-expression-arising-conflict-gaza-report

utilitzades de manera generalitzada a pràcticament tots els països analitzats com a eina per reduir al mínim o suprimir del tot la llibertat de premsa i censurar l'accés a pàgines web i mitjans de comunicació.

En aquest marc, hi ha els casos d'apagades digitals, que els Governs decreten especialment en moments d'agitació social i protestes massives, una tàctica gens innocent, després de la influència provada d'internet en l'expansió del malestar que va desembocar en les Primaveres Àrabs. Aquestes estratègies obstrueixen la capacitat dels moviments socials per organitzar-se i denunciar les vulneracions de drets humans, durant els esdeveniments clau, com les grans manifestacions. L'Iraq és un dels països que lideren aquesta estratègia política i digital, en què es registren un augment de la violència policial i de les milícies en les protestes que es van dur a terme durant els bloquejos d'internet.

2. ESTRATÈGIES I TECNOLOGIES DE VIGILÀNCIA MASSIVA

Les agències d'intel·ligència dels Governs del Maghreb i Mashreq segueixen utilitzant la intercepció de comunicacions com un dels principals instruments per a la vigilància de periodistes, defensores de drets humans i organitzacions de la societat civil. Tanmateix, aquests mecanismes s'han modernitzat amb l'adquisició de tecnologies avançades com programaris espia que entren als dispositius mòbils i ordinadors per sostreure'n informació rellevant de WhatsApp o fotografies.[3]

La tecnologia que fa possible l'expansió d'aquesta dinàmica està proporcionada majoritàriament per un petit grup d'empreses, entre les quals es repeteixen algunes empreses occidentals com Hacking Team, Blue Coat i NSO Group. A través d'aquestes empreses, alguns Governs com el d'Israel, el Marroc o el Líban, entre d'altres, han desenvolupat àmplies campanyes de vigilància massiva per monitorar defensores de drets humans i accedir a la seva informació personal i política.

Paral·lelament, s'identifica com a nova tendència la introducció de la intel·ligència artificial en armes no autònomes per tasques que van des d'extraure i emmagatzemar informació sensible de la població (per exemple, a través del reconeixement facial[4]) a la programació de bombes a l'ofensiva contra Gaza, per augmentar-ne la capacitat letal. Els drons s'utilitzen cada vegada més per vigilar mobilitzacions a països com Egipte, el Territori Ocupat del Sàhara Occidental o els carrers de Jerusalem Est i Cisjordània.

3 Vegeu glossari

4 Vegeu glossari

3. ASSETJAMENT EN LÍNIA

Els Governs del Maghreb i el Mashreq són líders globals en campanyes de desinformació, en molts casos dirigides a atacar la reputació de les organitzacions de la societat civil i de persones defensores de drets humans. Aquests atacs en línia provenen d'exèrcits electrònics[5] formats per milers de bots, que apuntalen i intensifiquen l'assetjament quotidià a les persones crítiques dissidents. Aquest tipus de campanyes d'assetjament en línia, de vegades porten a la violència física i incrementen el risc per la vida i la integritat de les persones defensores. En aquest informe es recullen diversos casos d'agressions físiques i inclús assassinats precedits de campanyes d'assetjament en línia.

Internet s'ha convertit per a la societat civil en un espai tan útil i alliberador com potencialment perillós, a causa de les eines de monitoreig dels continguts digitals a la recerca de postures crítiques amb les accions dels Governs o altres forces polítiques als països. Però no són només les autoritats les qui utilitzen internet per rastrejar i castigar els missatges i publicacions de les defensores de drets humans, també hi ha altres actors (sindicats policials, forces parapolicials o milícies) que, com és el cas a Egipte o l'Iraq, lideren aquestes accions de rastreig i assetjament.

A vegades, aquesta tàctica fins i tot involucra el conjunt de la societat. Per exemple, a països com l'Iraq, les autoritats han establert plataformes per tal que la societat civil pugui denunciar continguts ofensius o que ataquen la "moral" del país. En concret, en el primer any de funcionament a l'Iraq, es van recollir 96 000 denúncies.

4. IMPACTES DIFERENCIALS

En termes de drets, aquests impactes no afecten tothom per igual, sinó que hi intervenen variables com el gènere l'orientació sexual, la classe social i l'estatus legal. Es percep una tendència creixent a exposar, assetjar i vigilar les dones que trenquen amb els estereotips de gènere tradicionals i alcen les veus per criticar la reducció de l'espai democràtic, la falta de drets o l'ocupació militar. Aquesta situació deriva en el seu sotmetiment a tipus de violència específics, com la violència sexualitzada, l'expressió misògina a les xarxes socials, la publicació d'informació privada, com el seu contacta i l'adreça (pràctica que es coneix com a dòxing) o els atacs a l'honor. Aquestes dinàmiques de coerció s'acarnissen també amb altres grups vulnerabilitzats com les persones LGBTIQ+, que en bona part dels països analitzats estan sotmeses a la pràctica coneguda com a "enrampament", és a dir, emboscades a través d'aplicacions de contactes o bé pel carrer per poder-los acusar de vulnerar els articles legals que prohibeixen les relacions amb persones del mateix sexe.

5 Vegeu glossari

També forma part d'aquesta dinàmica l'exposició no consentida de l'orientació sexual, l'anomenat "*outing*"[6]; una pràctica que pot elevar el risc que les persones que en són objecte estiguin sotmeses a més violències.

La repressió que aprofita les desigualtats estructurals de gènere, impacta també en alguns homes. És el cas dels periodistes marroquins referenciats a l'informe, que es van veure immersos en processos judicials on se'ls feien acusacions molt greus, com els càrrecs de violació, per minar el potencial suport social que poden rebre quan són perseguits per publicar reportatges i articles crítics i incòmodes pel poder.

La criminalització creixent de la migració i la deshumanització de les persones migrants que travessen els països de la regió, en el seu camí cap a Europa (amb la Unió Europea que deslocalitza el control de fronteres a aquests països, a canvi de paquets econòmics) té també el seu vessant tecnològic. A més de ser objecte d'assetjament i difamació a través de mitjans digitals i xarxes socials, les persones migrants són el subjecte sobre el qual s'assagen tecnologies controvertides com ara la biometria. En casos com el del Líban, és habitual la confiscació de mòbils, ordinadors i altres mitjans de comunicació a camps de persones refugiades sirianes, fet que accentua l'aïllament social que ja pateixen aquestes persones.

Finalment, cal destacar l'impacte diferencial que la vigilància massiva té sobre les poblacions que viuen sota ocupació, com la palestina i la sahrauí. Bona part de les tecnologies identificades es desenvolupen i testegen sobre el poble palestí, que viu sota l'ocupació militar israeliana. Mentre que el Marroc s'ha convertit en un actor fonamental per al desenvolupament del sector a la regió. L'ecosistema empresarial es beneficia de la persistència d'aquestes ocupacions i del genocidi contra el poble palestí.

Res fa pensar que aquestes tendències a un augment accelerat del control i la vigilància sobre la població s'hagin de revertir en els pròxims anys, sobretot si es té en compte la creixent debilitat del sistema internacional de protecció dels drets humans. Per això, és imprescindible generar eines d'anàlisi i autodefensa per a les veus crítiques i les persones defensores de drets humans a tot el món i, en aquest cas, a la franja sud de la regió mediterrània. Amb aquest informe es pretén contribuir a aquest propòsit: conèixer el fenomen, els efectes que té sobre les persones defensores de drets humans i fer visibles les empreses implicades. Aquest és el primer pas per construir aliances de resistència i col·laboració, així com desenvolupar estratègies de protecció i incidència política. Estratègies que també han de servir per establir mecanismes de control per a les empreses involucrades i exigir que els Governs garanteixin els drets humans en l'ús de les tecnologies.

6 Vegeu glossari

RECOMANACIONS

Les següents recomanacions sorgeixen de les principals conclusions d'aquest informe, així com de l'anàlisi de les pràctiques internacionals, estudis de casos i recomanacions de diverses organitzacions de drets humans. L'objectiu és proporcionar un marc integral per prevenir els riscos de la vigilància massiva i protegir la democràcia i l'espai cívic.

Totes les recomanacions van dirigides a totes les institucions (Governs municipals i regionals, Estats, Unió Europea i Nacions Unides).

1. PROHIBICIÓ I REGULACIÓ DE TECNOLOGIES INTRUSIVES

- Moratòria sobre l'exportació i l'ús de tecnologies de vigilància. Els Estats han d'establir immediatament una moratòria sobre la venda, transferència i ús de la tecnologia de vigilància. Hi ha una necessitat urgent d'aturar les activitats que es duen a terme mitjançant tecnologies de vigilància de tots els Estats i empreses, fins que els marcs reguladors assegurin el respecte dels drets humans.
- Prohibició total de la vigilància massiva biomètrica. Els Estats han de prohibir l'ús total, el desenvolupament, la producció, la venda i l'exportació de tecnologies de reconeixement facial i altres formes de vigilància biomètrica, sense excepcions.
- Prohibició de tecnologies provades en contextos de conflictes. Cal que els Estats prohibeixin l'ús, el desenvolupament i l'exportació de tecnologies de vigilància provades en conflictes armats o en contextos d'ocupació de poblacions civils.
- Prohibició de l'ús de tecnologies d'alt risc per als drets fonamentals. Els Estats han de prohibir en tots els casos el perfilatge automatitzat, el reconeixement d'emocions i la categorització biomètrica en procediments d'asil i contextos migratoris, així com en qualsevol tipus de procés que pugui tenir impacte sobre els drets fonamentals de les persones, com pot ser en el marc d'una investigació policial.
- Prohibició de l'ús de programari espia i protecció de drets. Els Estats han d'aprovar nous marcs jurídics que abordin els desafiaments que planteja el programari espia, que incloguin una prohibició de la producció, exportació, venda, importació, adquisició, transferència, manteniment i ús del programari espia, perquè interfereix de manera desproporcionada amb els drets fonamentals i encara no hi ha salvaguardes adequades per prevenir i reparar els danys als drets humans.
- Garantir programes d'I+D lliures de tecnologia intrusiva. Les institucions han d'assegurar que els programes d'I+D no col·laboren amb empreses vinculades al desenvolupament de tecnologies de vigilància, incloses les de l'àmbit militar.

2. TRANSPARÈNCIA I RESPONSABILITAT EN LA CONTRACTACIÓ I ÚS DE TECNOLOGIES DE VIGILÀNCIA

- Transparència i auditoria de contractes públics. Les institucions han d'assegurar l'existència i la implementació de mecanismes de control i auditoria de les contractacions públiques de tecnologia. S'han d'incloure en la contractació pública avaluacions d'impacte sobre drets fonamentals a càrrec de l'empresa prestadora del servei, amb l'objectiu d'evitar afectacions als drets fonamentals abans de la posada en marxa del servei. En aquesta avaluació s'han d'incloure possibles mesures de mitigació i fins i tot de reparació en el cas que hi hagi afectacions. Es podrien incloure mecanismes de reclamació davant les autoritats de contractació perquè puguin rebre queixes de manera efectiva relacionades amb els efectes negatius sobre els drets humans, vinculats o causats per l'empresa prestatària del servei.
- Transparència i avaluació de riscos. Les autoritats han de dur a terme avaluacions de risc i impacte en els drets humans, abans d'adquirir i implementar tecnologies de vigilància i incorporar mecanismes de participació de la societat civil i grups potencialment afectats i altres actors amb coneixement tècnic. Les empreses tecnològiques han de proporcionar transparència sobre les seves tecnologies, incloent-hi informació sobre la gestió de riscos que realitzen, informació sobre les dades amb les quals s'ha entrenat la tecnologia —si inclou entrenament de dades— i les mesures de governança de dades que han implementat per evitar biaixos. També han de permetre auditories dels seus algoritmes, en un marc que garanteixi un nivell suficient de confidencialitat.
- Contractació pública d'empreses militars amb fins vinculats a la vigilància. Les institucions han de garantir que l'accés de les empreses militars a contractacions públiques estigui subjecte a estrictes estàndards de drets humans i que s'excloguin les empreses involucrades en violacions greus. Han de promoure el compliment de normes internacionals com l'Arranjament de Wassenaar i fomentar la transparència en el comerç de tecnologies de vigilància.

3. PROTECCIÓ DELS DRETS DIGITALS: PRIVACITAT I LA PROTECCIÓ DE DADES

- Protecció de dades personals i privacitat. Les institucions han de garantir que les tecnologies utilitzades respectin els drets de privacitat i la protecció de dades.
- Protecció de la privacitat i ciberseguretat. Les legislacions que regulen la privacitat electrònica han d'incloure proteccions més estrictes per a la confidencialitat de les comunicacions i el dret a la protecció dels dispositius.
- Sobre la vigilància comercial. Les institucions han d'establir una regulació clara que limiti les pràctiques de vigilància comercial i protegeixi la privacitat de les consumidores. Això inclou la prohibició de la recopilació de dades, sense el consentiment explícit de les usuàries i la implementació de mecanismes de transparència que permetin a les consumidores conèixer com s'utilitzen les seves dades. És necessari reforçar la legislació que estableix salvaguardes per a l'accés de les Forces i Cossos de Seguretat de l'Estat (FFCCSE) a les dades d'empreses (e-evidence).

4. RENDICIÓ DE COMPTES, PARTICIPACIÓ DE LA SOCIETAT CIVIL I ACCÉS A LA JUSTÍCIA

- Foment del debat públic sobre vigilància digital. Les institucions han d'assegurar la participació de la societat civil de forma regular i significativa per debatre sobre el disseny i ús de tecnologies de vigilància, així com el seu impacte en les llibertats civils i els drets humans.
- Rendició de comptes i reparació. Les institucions han d'eliminar els obstacles que impedeixen a les víctimes de vigilància massiva accedir a la justícia i garantir investigacions policials i judicials ràpides, efectives i transparents. Les víctimes han de tenir accés a la informació intervinguda i mecanismes de reparació. La societat civil ha de participar en tot el que té a veure amb l'ús de tecnologies de vigilància, de manera regular i significativa des de la fase de disseny, implementació, supervisió i control, així com també des dels processos de contractació pública. Han d'existir mecanismes de transparència i accés a la informació sobre aquestes tecnologies, com ara l'existència de registres públics perquè la població pugui conèixer on estan implementades aquestes tecnologies.

5. COOPERACIÓ I HARMONITZACIÓ INTERNACIONALS

- Creació d'un grup de treball sobre vigilància digital. Les institucions han d'establir grups de treball especialitzats per supervisar i analitzar els abusos provocats per la vigilància digital, des de l'escala local fins a la global i proposar recomanacions per mitigar aquests abusos.
- Extraterritorialitat en la legislació. Les institucions han d'incloure el principi d'extraterritorialitat a totes les regulacions relacionades amb la vigilància massiva.
- Reformes legislatives i participació de la societat civil: Cal que les institucions reformin les lleis de seguretat, per ajustar-les als estàndards de protecció de drets individuals i col·lectius i garantir la participació de la societat civil en els processos legislatius.
- Obligacions en matèria de drets humans. L'externalització de poders de vigilància a empreses provades no eximeix els Estats i administracions de les seves obligacions en matèria de drets humans.
- Compliment dels Principis Rectors sobre Empreses i Drets Humans del Consell de Drets Humans. Les empreses han d'operar de manera que respectin els drets humans en totes les seves activitats i minimitzin el risc d'abús. Els Estats han d'establir regulacions i polítiques per assegurar que les empreses tecnològiques compleixen amb aquests principis de respecte, prevenció i responsabilitat envers els drets humans. Els Estats han d'incloure en els seus marcs normatius mecanismes de reparació també alineats amb els Principis Rectors.

6. REGULACIÓ I SUPERVISIÓ DE LES EMPRESES QUE DESENVOLUPEN, INCORPOREN I UTILITZEN TECNOLOGIA DE VIGILÀNCIA

- Responsabilitat i diligència deguda en drets humans. Les empreses de vigilància i aquelles que recopilen dades de manera massiva han d'integrar la diligència deguda, en matèria de drets humans en totes les etapes de desenvolupament dels seus productes i mantenir involucrada la societat civil de manera significativa.
- Auditories i transparència. Les empreses han de dur a terme auditories anuals externes per avaluar l'impacte dels seus productes sobre els drets humans i facilitar l'accés als investigadors per supervisar riscos sistemàtics.
- Inversions respectuoses amb els drets humans. S'insta a les persones i entitats inversores a adoptar principis d'inversió ètica que prioritzin el respecte als drets humans en les seves decisions.

7. REFORÇ DE LA SOBIRANIA TECNOLÒGICA

- Interoperabilitat i alternatives. Els Estats han de garantir que les persones poden triar alternatives respectuoses amb els drets, enfront de les plataformes tecnològiques dominants i exigeixin interoperabilitat entre aquestes plataformes.
- Normes de contractació pública. Els Estats han d'establir criteris que prioritzin la transparència i l'ètica en la selecció de proveïdors que compleixin amb els estàndards de drets humans.
- Codi Obert. Els Estats han de fomentar l'ús de programari de codi obert per garantir l'auditoria i l'accés públic a les eines utilitzades en la recopilació i anàlisis de dades i promoure la transparència i la confiança.
- Finançament públic. Els Estats han de dedicar fons públics a iniciatives que se centrin en la recopilació ètica de dades i prioritzin projectes que protegeixin la privacitat dels usuaris i promoguin un ús responsable de la tecnologia.

ANNEXOS

1. GLOSSARI

- **Amenaces Persistents Avançades (APT):** Tècniques sistemàtiques de pirateig per a accedir a un sistema digital i romandre-hi durant un període prolongat, amb finalitats malicioses com ara la sostracció de dades personals.
- **Atac DDoS:** Un atac DDoS (Distributed Denial of Service) és un tipus de ciberatac que busca interrompre el funcionament d'un lloc web o servei en línia. Això s'aconsegueix sobrecarregant el servidor amb una gran quantitat de sol·licituds d'accés simultànies, enviades des de múltiples dispositius o "bots" infectats. Aquesta afluència massiva de trànsit pot alentir el lloc web o, fins i tot, fer que deixi de funcionar temporalment, impedint l'accés a usuaris legítims.
- **Atacs zero-clic o injeccions en xarxa:** tècniques de programari espia que permeten infiltrar un dispositiu, sense necessitat d'interacció per part de l'usuari afectat.
- **Comportament inautèntic Coordinat (*Astroturfing* o falsificació de corrents d'opinió):** emmascarament de l'organització i direcció d'una campanya coordinada perquè sembli que sorgeix espontàniament de la població i de la societat civil.
- **Data breach**: accés i robatori d'informació sensible o confidencial per mitjans il·lícits o il·legals.
- **Inspecció Profunda de Paquets (DPI - Deep Packet Inspection):** un tipus de processament de dades usat per a moltes funcions, entre d'altres, el control, filtrat i bloqueig de l'activitat a internet, en temps real i de manera dirigida.
- ***Doxxing* o dòxing:** publicar informació personal i documents audiovisuals d'una persona sense el seu consentiment.
- **Exèrcit Electrònic:** grup de pirates informàtics que dona suport a les accions d'un determinat Govern, la missió del qual és utilitzar Internet, xarxes socials i atacs cibernètics per a lluitar contra els adversaris polítics.
- **Emboscada o entrampament digital**: enganyar a algú perquè cometi un crim (segons les lleis del país) en els espais digitals.
- **Extorsió digital o cibernètica:** és una forma de delicte informàtic, en la qual hi ha individus que fan xantatge digitalment a organitzacions o persones, per a obtenir allò que volen. Poden amenaçar de filtrar dades, llançar atacs cibernètics, deshabilitar operacions, evitar que els usuaris accedeixin a les dades o, fins i tot, arribar a destruir les dades obtingudes.

- ***Fake news* o notícies falses:** difusió de notícies falses o faules, amb l'objectiu de crear un estat d'opinió particular, confondre i desinformar a l'audiència.
- **Granja o fàbrica de trolls (o *trolling* online):** pot ser un grup de comptes automàtics (bots) o persones pagades per influenciar l'opinió pública, a través de les xarxes socials, sobre temes polítics o d'actualitat.
- ***Malware* o programari maliciós:** qualsevol tipus de programa o codi dissenyat per danyar, explotar o infiltrar-se en sistemes informàtics, sense el consentiment de la usuària.
- ***OAuth Phishing (Open Authorisation Phishing):*** modalitat del *phishing* o pesca, en la qual s'enganya als usuaris perquè atorguin permisos a aplicacions malicioses que poden accedir a les dades del seu compte i realitzar accions en el seu nom.
- ***Outing*:** fer pública la identitat sexual o de gènere d'una persona, sense el seu consentiment.
- ***Phishing* o pesca:** aquesta tècnica informàtica consisteix a fer-se passar per una persona, empresa o servei de confiança per a enganyar a una víctima, guanyar-se la seva confiança per a estafar-la o vigilar les seves comunicacions.
- **Reconeixement facial:** identificació biomètrica de la identitat d'una persona, a partir de certs punts físics de la cara.
- ***Spyware* o programari espia:** un tipus de *malware* o programari maliciós que, encara que pot no danyar l'ordinador, controla i espia d'amagat totes les accions que es realitzen a través de l'ordinador infectat.
- ***Trojan Horse* o virus troià:** un tipus de programari maliciós que s'amaga darrere un altre arxiu, aparentment innocu, per accedir a algun sistema, sense ser detectat. Hi ha molts tipus de troians (un exemple és el *backdoor trojan*, que obre accés per proporcionar el control remot d'un ordinador).

2. DIRECTORI
d'empreses de vigilància massiva operant en el Maghreb i Mashreq

- **AGT (Advanced German Technologies):** empresa amb seu a Dubai. Es dedica principalment a la revenda d'equips forenses digitals i serveis de tecnologia de vigilància. La seva tecnologia ha estat utilitzada a Síria.[1]
- **Amesys (*Advanced Middle East Systems*):** empresa francesa sota el control de la també francesa Bull. Amesys va desenvolupar el sistema Eagle System de vigilància digital massiva de trànsit amb funcions de censura (a través de Deep Packet Inspection). El 2015 Amesys passa a dir-se Nexa Technologies i crea un nou sistema de vigilància massiva amb el nom de "Cervell", amb capacitat de rastrejar telecomunicacions a temps real. Ha estat utilitzada al **Marroc**[2] i **Egipte**.[3]
- **Anyvision:** empresa israeliana especialitzada en reconeixement facial a través de cambres intel·ligents. La tecnologia d'aquesta empresa s'utilitza en punts de control militar israelià contra la població en **Palestina**.[4]
- **AREA SpA:** empresa italiana que, en col·laboració amb Utimaco i Qosmos, ha participat en el desenvolupament d'un sistema central de monitoratge utilitzat per al control i la vigilància de la població **siriana**,[5] liderat per Syrian Telecom.

---

1 **Franceschi-Bicchierai, Lorenzo.** "European Surveillance Companies AGT and RCS Sell Syria Tools of Oppression." Vice. 12 de desembre del 2016.
Disponible a:
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 novembre del 2017.
Disponible a: https://reflets.info/articles/maroc-popcorn-le-projet-qui-n-existait-pas

3 T**esquet, Olivier.** "Amesys: Egyptian Trials and Tribulations of a French Digital Arms Dealer." Télérama, 5 de juliol del 2017.
Disponible a:
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 a: 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 a:
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 i especialitzada en la producció de drons de vigilància i reconeixement. Els drons Bayraktar TB2 han estat utilitzats en els conflictes de Líbia, **Síria** i l'Alt Karabakh. El 2021, el **Marroc** ha utilitzat els seus drons per a activitats de reconeixement al **Sàhara Occidental**.[6]

- **Blue Bird Aero Systems:** empresa israeliana especialitzada en el disseny i producció de drons des de 2002. Israel Aerospace Industries és propietària el 50 % de les seves accions. Actualment, al **Marroc**,[7] hi ha una planta de producció dels drons tipus WanderB i ThunderB especialitzats en missions de reconeixement i vigilància.

- **Blue Coat Systems:** empresa nord-americana adquirida en 2016 per Symantec. Posteriorment Symantec va ser absorbida per l'empresa californiana Broadcom, el 2019. Des de llavors, desapareix la marca Blue Coat, però els seus sistemes continuen sent utilitzats per Broadcom. La seva tecnologia va servir per a interceptar i inspeccionar dades de les xarxes de telecomunicacions per a la vigilància massiva de dispositius mòbils, ordinadors, interaccions a les xarxes socials, correus electrònics i comunicacions en línia. Aquests sistemes van ser adquirits i utilitzats pels Governs de **l'Iraq**,[8] **Líban**,[9] **Síria**[10] i **Tunísia**.[11]

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

7 A**ublanc, Alexandre.** "Morocco to Become Rare Military Drone Manufacturer Thanks to Cooperation with Israel." Le Monde. 9 de maig del 2024.
Disponible a:
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 C**itizen 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 de gener del 2013.
Disponible a:
https://citizenlab.ca/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest

10 **The Citizen Lab.** "Behind Blue Coat." 2011.
Disponible a: 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.º 93. 8 de juliol del 2014.
Disponible a: https://journals.openedition.org/conflits/18863

- **Circles:** empresa de cibervigilància israeliana creada el 2011. Tant NSO Group com Circles estan sota el control de l'empresa de capital d'inversió tecnològica nord-americana Francisco Partners. La seva tecnologia s'especialitza en la identificació de vulnerabilitats en les xarxes de comunicació per interceptar trucades, textos, monitorar ubicacions de dispositius mòbils, entre d'altres. **Israel** i el **Marroc**[12] haurien utilitzat aquesta tecnologia.

- **Cognyte:** empresa israeliana especialitzada en solucions de ciberseguretat. La seva tecnologia de recerca s'utilitza per a identificar amenaces de seguretat a les esferes analítiques. No obstant això, el seu programari ha estat utilitzat al **Marroc**[13] [14] per crear i gestionar comptes falsos a les xarxes socials com Facebook, Instagram, Twitter, YouTube o VKontakte.

- **Corsight AI:** empresa israeliana especialitzada en reconeixement facial. La canadenca Awz és propietària d'aquesta empresa. Els serveis d'intel·ligència israelians i la Unitat 8200, utilitzen aquesta tecnologia per vigilar la població **palestina**.[15]

- **Cytrox:** companyia creada el 2017, amb seu oficial a Macedònia del Nord, però operada des d'Hongria i Israel. És cèlebre pel seu programari maliciós usat per a ciberatacs i vigilància encoberta. Cytrox forma part de Intellexa Consortium, un grup d'empreses de programari espia. El seu producte Cytrox Predator ha estat utilitzat a **Egipte**[16] contra opositors polítics i periodistes.

- **Dahua Technologies:** empresa amb seu en Hangzhou, la Xina, especialitzada en el disseny i producció de tecnologies de vigilància i seguretat. Les seves càmeres de lectura de matrícules de vehicle, reconeixement facial i detecció de moviment es troben en el **Territori Ocupat de Palestina**.[17]

---

12 **Citizen Lab.** "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." 1 de desembre del 2020. Disponible a:
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 setembre del 2024.
Disponible a: https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/

14 **Mike Dvilyanski, David Agranovich y Nathaniel Gleicher.** "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 de desembre del 2021.
Disponible a:
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 març del 2024.
Disponible a: 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 setembre del 2023.
Disponible a:
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. Novembre del 2022.
Disponible a:
https://www.whoprofits.org/writable/uploads/old/uploads/2018/11/surveil-final.pdf

- **ETI:** empresa danesa especialitzada en ciberseguretat i cibervigilància que el 2011 va ser adquirida per la multinacional alemanya BAE Systems. ETI va desenvolupar el programari Evident i X-Stream per rastrejar els hàbits de navegació de les usuàries d'internet, desencriptar i interceptar crides i correus electrònics. El **Marroc**[18] ha adquirit aquesta tecnologia. A **Tunísia**,[19] a més, s'ha identificat l'ús d'aquesta tecnologia per a reprimir opositors, durant el règim de Ben-Ali.

- **Gamma Group:** empresa britànica especialitzada en ciberseguretat i el desenvolupament de solucions tecnològiques de vigilància. Un dels seus principals productes és el programari espia FinFisher o FinSpy que pot ser usat per infectar ordinadors i dispositius mòbils, amb la finalitat de sostreure'n de dades. S'ha trobat tecnologia FinFisher en una sofisticada infraestructura de ciberespionatge, coneguda com a Dark Caracal, vinculada als serveis d'intel·ligència del **Líban**[20] **Egipte**[21] i el **Marroc**[22] també van adquirir aquesta tecnologia per a la intercepció de telecomunicacions.

- **Guàrdia Systems:** empresa libanesa, que forma part del MG Holding Group. Guàrdia està especialitzada en el desenvolupament de solucions tecnològiques en el sector de la ciberseguretat per a empreses extractivistes, Governs i infraestructures crítiques. L'any 2016 va instal·lar, a Beirut, al **Líban**,[23] sistemes de càmeres de videovigilància, amb capacitat de lectura i registre de matrícules de vehicles, així com sistemes de vigilància a **l'Iraq**.[24]

---

18 **BBC News.** "Israel to Set Up New Military Unit to Combat Hamas Cyber Threats," 21 de juny del 2017.
Disponible a: 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 gener del 2018.
Disponible a: https://thehackernews.com/2018/01/dark-caracal-android-malware.html

21 **Amnistia Internacional.** "German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed," Amnesty International, 25 de setembre del 2020.
Disponible a:
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 d'octubre del 2015.
Disponible a:
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 a:
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 d'octubre del 2023.
Disponible a:
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, ja desapareguda, coneguda pel desenvolupament del programari de vigilància massiva Remote Control System. Aquest programari espia permetia capturar dades de mòbils i comunicacions en plataformes com Skype, així monitorar la localització per GPS dels dispositius. La seva tecnologia va ser adquirida pels serveis d'intel·ligència del **Marroc**[25] i el **Líban**[26] i ha servit per perseguir defensores de drets humans i periodistes.

- **Hikvision:** empresa multinacional xinesa líder en solucions de videovigilància. Les càmeres de detecció de moviment i reconeixement biomètric es troben a **Tunísia**[27] i a **Jerusalem**.[28]

- **Idemia:** multinacional francesa especialitzada en sistemes d'identificació biomètrica automatitzada. Anteriorment coneguda com a Morpho, forma part d'Advent International des del 2017, un fons de capital privat. El seu producte MBIS, que permet obtenir empremtes dactilars, petjades de la palma i trets facials, ha estat venut recentment al Govern de **Tunísia**[29] per reforçar la seguretat de les fronteres.

- **Indra Sistemas:** empresa espanyola, amb participació pública, especialitzada en solucions tecnològiques per al sector de la defensa i ciberseguretat a escala global i amb participació pública entre els seus accionistes. El 2019, va contribuir a expandir la xarxa de vigilància per satèl·lit per controlar l'espai aeri del sud del **Marroc** i el **Sàhara Occidental**,[30] mitjançant la instal·lació de sistemes avançats de comunicacions i vigilància.

---

25 **Citizen Lab.** "Backdoors Are Forever: Hacking Team and the Targeting of Dissent," Citizen Lab, 7 'octubre del 2012.
Disponible a:
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 juliol del 2015.
Disponible a:
https://smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

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

28 **Amnistia Internacional.** "Israeli Authorities Are Using Facial Recognition Technology to Entrench Apartheid," 24 de maig del 2023.
Disponible a:
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 març del 2024.
Disponible a:
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 a: https://www.odhe.cat/es/indra-sistemas-s-a/

- **Inmobiles:** empresa libanesa, subsidiària de la britànica Resource Holding Group, que aporta sistemes de captura biomètrica per registrar usuaris que compren dispositius mòbils al **Líban**, d'acord amb el registre de mòbils (International Mobile Equipment Identity - IMEI).[31]
- **IrisGuard:** empresa britànica fundada el 2011 i especialitzada en solucions biomètriques. Entre els seus propietaris, hi ha diversos fons d'inversió com GrowthGate Capital. Els seus sistemes d'identificació biomètrica s'utilitzen per a registrar a les refugiades sirianes que sol·liciten ajuda a les agències de Nacions Unides a **Jordània**.[32]
- **Magal Security Systems:** empresa israeliana líder global de sistemes perimetrals. Creada el 1969 a partir de l'empresa pública Israeli Aerospace Industries (IAI). Des d'aleshores, ha aportat sistemes de tancat intel·ligent, amb sensors de detecció de moviment i càmeres de videovigilància modernes per als assentaments il·legals i el mur de l'Apartheid d'Israel a **Palestina**.[33]
- **Mer Group:** empresa israeliana especialitzada en sistemes de vigilància massiva. La seva tecnologia es troba en el projecte Mabat 2000, per a la vigilància de la ciutat vella de **Jerusalem** i el control de la població **palestina**.[34]
- **MSAB (Mycro Systemation AB):** empresa tecnològica de nacionalitat sueca, líder mundial en extracció i anàlisi de dades de mòbils. L'empresa franc-libanesa Intertech va subministrar aquesta tecnologia al **Marroc**. El **Marroc**[35] podria haver utilitzat aquesta tecnologia per perseguir a la dissidència política i les defensores de drets humans, ja que no hi ha controls sobre l'ús d'aquesta tecnologia (que va ser transferida per la UE per al control de fronteres).

31 **SMEX.** "Ministry of Telecommunications IMEI Registration Policy Threatens Digital Privacy," 4 de desembre de 2018.
Disponible a:
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 d'abril del 2021.
Disponible a: 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 a: https://novact.org/wp-content/uploads/2023/10/Informe_Muros-invisibles_ocupacion.pdf

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

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

- **MTN Syria:** proveïdor de serveis mòbils, subsidiària de l'empresa sud-africana MTN. MTN ha donat suport al Govern **sirià**[36] pel que fa al filtratge i bloqueig de les telecomunicacions dels seus usuaris.

- **NSO Group:** empresa israeliana amb seu a Herzliya, especialitzada en el desenvolupament de programari espia per monitorar i interceptar dades de dispositius mòbils. El seu producte més conegut, el programari espia Pegasus, és capaç de sostreure dades de correus electrònics, trucades i imatges i activar la càmera dels mòbils, fins i tot, sense necessitat d'interacció per part de l'usuari afectat. Pegasus ha estat adquirit pel **Marroc**, el **Líban**, **Jordània** i **Israel** i ha estat usat per a espiar líders polítiques, periodistes i defensores de drets humans. Les autoritats marroquines i israelianes també han utilitzat el programari espia Pegasus per vigilar i controlar la població civil **palestina** i **sahrauí**.[37]

- **Oxygen Forensics:** empresa especialitzada en informàtica forense, amb seu a Virgínia, els Estats Units. Un dels seus principals productes tecnològics és l'Oxygen Forensic Detective que té capacitat d'anàlisi i extracció de dades de mòbils. Les autoritats marroquines van accedir a aquesta tecnologia el 2022, a través de l'empresa francolibanesa Intertech. El **Marroc**[38] podria haver utilitzat aquesta tecnologia per perseguir la dissidència política i les defensores de drets humans, ja que no hi ha controls sobre l'ús d'aquesta tecnologia (que va ser transferida per la UE per al control de fronteres).

- **Palantir Technologies:** empresa creada el 2003, amb seu a Denver, als Estats Units, s'especialitza en l'anàlisi de dades i programaris amb IA. L'exèrcit israelià utilitza la seva tecnologia per a les seves operacions militars a **Palestina**.[39]

- **Qosmos:** companyia francesa que va subministrar l'empresa de Telecomunicacions de **Síria**,[40] STE, eines d'inspecció profunda de paquets (DPI), projecte que va finalitzar el 2012.

---

36 **Digital Dominion Report.** 2021.
Disponible a: 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 gener del 2022.
Disponible a: 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 juliol del 2022.
Disponible a: https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware

39 **American Friends Service Committee.** "Palantir Technologies".
Disponible a: 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 a:
https://www.ecchr.eu/en/case/surveillance-in-syria-european-firms-may-be-aiding-and-abetting-crimes-against-humanity/

- **Grup Safran:** multinacional francesa creada el 2005 per empreses del sector de defensa. Safran va participar, juntament amb altres empreses com Motorola, Northrup Grumman o L-1, en el desenvolupament del Sistema Automatitzat d'Identificació Biomètrica (ABIS, per les seves sigles en anglès) per al registre i sistematització de dades biomètriques de la població de **l'Iraq** i **l'Afganistan**.[41] El 2009, el Ministeri de Comunicacions de **l'Iraq**[42] va contractar Safran per desenvolupar un sistema de monitoratge d'internet i bloqueig de pàgines web.

- **Sandvine:** empresa canadenca especialitzada en la inspecció profunda de paquets (DPI). En el cas **d'Egipte**,[43] aquesta tecnologia s'ha fet servir per tancar més de 600 mitjans crítics o webs d'organitzacions de defensa dels drets humans, fet pel qual ha entrat en un llistat del Departament del Tresor dels Estats Units.

- **Thales Group:** multinacional francesa del sector aeroespacial, defensa, seguretat i identitat digital, creada el 1893 i amb participació del Govern francès. De manera directa, o a través de la seva subsidiària Gemalto, ha aportat tecnologia que s'ha utilitzat per a la captura de dades biomètriques en documents d'identificació al **Líban**[44] i el **Marroc**.[45] També s'identifiquen contractes amb el Ministeri de Comunicacions de **l'Iraq**,[46] sobre sistemes de vigilància.

- **TKH Group:** empresa tecnològica amb seu als Països Baixos que s'especialitza en el desenvolupament de sistemes de vigilància, comunicacions i connectivitat. La seva subsidiària TKH Security Solutions, ven càmeres de vigilància, sota el seu propi nom i la marca Grundig, a la policia **israeliana** i als assentaments il·legals israelians. A partir del 2023, s'han instal·lat diverses càmeres de circuit tancat de televisió de TKH Security i Grundig per a la vigilància policial i altres infraestructures de les zones residencials de **Jerusalem Est**.[47]

---

41 **Nina Toft Djanegara.** "Biometrics for Counter-Terrorism: Case Study of the U.S. Military in Iraq and Afghanistan," Privacy International. Juny 2021.
Disponible a:
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 a: 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 del 2024.
Disponible a: 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 a: https://www.thalesgroup.com/en/countries/middle-east-and-africa/thales-morocco

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

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

- **Total Secure Defence (TSA):** empresa amb seu als Emirats Àrabs Units i proveïdora de sistemes i equipament de seguretat. Al **Marroc**[48] s'han adquirit els seus productes com ara sistemes de vigilància i IMSI Catchers (dispositius que enganyen els dispositius mòbils per obtenir tota la informació relacionada amb el telèfon), que es fan servir per interceptar dades de telecomunicacions en temps real.

- **Trovicor:** inicialment creada com un departament d'intel·ligència de Siemens. A partir del 2009, és adquirida per un fons d'inversió i es constitueix com a empresa amb seu a Dubai. El 2019 va seriosament adquirida per la francesa Boss Industries. Trovicor s'especialitza en serveis d'intel·ligència i ciberseguretat. El règim de Ben-Ali va adquirir els seus sistemes d'intercepció, anàlisi de dades de telecomunicacions i rastreig de localitzacions de dispositius mòbils de la societat civil de **Tunísia**.[49]

- **Utimaco:** empresa de ciberseguretat amb seu a Alemanya i als Estats Units. En 2021 va ser adquirida pel fons SGT Capital. Els règims d'Al-Assad, a **Síria**,[50] i de Ben Ali, a **Tunísia**[51] va fer servir aquesta tecnologia per reprimir les revolucions àrabs, a través d'un sistema de vigilància vinculat amb la xarxa de telecomunicacions. En el cas de Síria, Utimaco va cooperar també amb l'empresa italiana Area Spa i la francesa Qosmos SA.

- **URS:** empresa nord-americana fundada el 1951 i especialitzada en serveis tècnics d'enginyeria i construcció. En 2014, va passar a estar sota el control de la també nord-americana AECOMS. EL 2018 URS va aportar sistemes de càmeres de videovigilància modernes amb alta resolució, llarg abast, detecció tèrmica i de moviment al mur fronterer entre **Tunísia** i **Líbia**.[52] [53]

---

48 **Total Secure Defence.** "IMSI Catchers and Interception Systems in Morocco," Total Secure Defence. Disponible a: 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 del 2012. Disponible a: 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?". Disponible a: 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 a: https://www.privacyinternational.org/state-privacy/1012/state-surveillance-tunisia

52 **Kapitalis.** "Des Américains installent la surveillance électronique au sud de la Tunisie," 14 d'agost del 2016. Disponible a: 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 febrer del 2021. Disponible a: https://www.africaintelligence.com/north-africa/2021/02/12/washington-consolidates-tunisia-libya-electronic-border-surveillance-wall,109642877-art

- **VASTech:** empresa amb seu a Sudàfrica que, en associació amb AGT, ha subministrat diverses tecnologies d'intercepció de les comunicacions a **Síria.**[54]
- **Veridos:** empresa amb seu a Berlín que sorgeix de la fusió, el 2014, de dues empreses alemanyes líders en el sector de la tecnologia de seguretat i identitat digital Giesecke+-Devrient i Bundesdruckerei. El 2016 inicien la implementació d'un sistema de reconeixement biomètric per al control de fronteres al **Marroc.**[55]

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

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