VIGILÀNCIA MASSIVA AL MAGHREB I EL MASHREQ

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

RESUM EXECUTIU

En les últimes dècades, el desenvolupament tecnològic i la digitalització han facilitat l'aparició de noves tècniques de vigilància i control cada vegada més esteses i intrusives, que plantegen nous reptes per a la protecció dels drets humans. Aquest informe analitza la manera en què, a la regió del Maghreb i Mashreq, els governs i les empreses utilitzen tecnologies avançades de vigilància digital per a controlar i reprimir la societat civil, fet que afecta de manera diferencial a persones migrants, dones i comunitat LGBTIQ+. Aquestes tecnologies, desenvolupades en gran part per empreses del Nord Global, han creat un context de vigilància massiva que amenaça drets fonamentals com la llibertat d'expressió, la privacitat i el dret a la informació. Les tecnologies emergents s'adquireixen en nom de la seguretat nacional i sota el pretext d'haver-se d'adaptar a noves formes de criminalitat, però restringeixen l'espai de participació política i intensifiquen el control social.

Aquest informe complementa l'anterior publicat, centrat en l'ús de la tecnologia de vigilància massiva a Europa. La combinació d'ambdós informes proporciona una visió de l'ús d'aquestes tecnologies i el seu impacte en la societat civil de la regió mediterrània.

L'informe analitza de manera específica la situació en 9 països de la regió:

- **El Marroc:** La repressió digital al Marroc inclou l'ús de *spyware* com Pegasus, i el *trolling* utilitzats per difamar i assetjar figures crítiques amb el sistema. Es vulnerabilitzen especialment els drets de les dones activistes i periodistes, que son objecte de campanyes de desprestigi amb connotacions misògines. Aquesta repressió està emparada per una legislació opaca i compta amb el suport de tecnologies intrusives subministrades per empreses del Nord Global.
- **Sàhara Occidental:** Després de la fi de la treva el 2020, la repressió i vigilància sobre la població sahrauí s'ha intensificat. Amb l'ajuda de tecnologia avançada, la col·laboració militar amb Israel i la implementació de drons i sistemes de vigilància digital, el Marroc ha imposat un control sever al Sàhara Occidental. Això afecta tant defensores de drets humans com periodistes sahrauís, especialment dones.

Aquesta estratègia ha creat un clima de repressió sistemàtica, ha forçat el desplaçament de la població civil i ha afectat drets fonamentals de moviment, privacitat i expressió, amb l'objectiu de consolidar el control sobre el territori ocupat.

- **Tunísia:** En estat d'emergència permanent, Tunísia manté pràctiques de vigilància heretades de la dictadura per controlar activistes, jutgesses, periodistes i persones LGBTIQ+, utilitzant lleis de ciberdelinqüència que permeten la recopilació de dades privades i el pirateig de dispositius. Més de 40 persones han estat detingudes pel seu activisme, sota la Llei de Ciberdelinqüència, alhora que la vigilància fronterera amb Líbia, finançada pel Nord Global, endureix la repressió contra persones migrants i reforça el control estatal.
- **Egipte:** El Govern egipci usa una xarxa de ciberespionatge avançada i fa servir programari espia, com *Cytrox's Predator*, i tecnologia de censura com la inspecció profunda de paquets (DPI), per interceptar comunicacions. També ha bloquejat més de 600 llocs web crítics amb el règim. La repressió digital inclou campanyes d'assetjament i difamació a les xarxes socials, dirigides a activistes, periodistes i defensores de drets humans, secundades per bots i comptes pro-govern, amb atacs homòfobs i misògins freqüents.
- **Líban:** Les agències d'intel·ligència duen a terme un monitoratge exhaustiu de les comunicacions de la societat civil, amb l'ús de tecnologies avançades, com el sistema de ciberespionatge Dark Caracal. La infraestructura digital al Líban és vulnerable, sent la major bretxa de seguretat al país el recent atac massiu d'Israel dirigit contra militants de Hezbollah mitjançant l'explosió dels seus dispositius, busques i walkie-talkies. L'Oficina de Ciberdelinqüència actua per a silenciar periodistes, activistes i blogueres mitjançant l'ús de lleis restrictives, fet que fomenta l'autocensura i el tancament de continguts digitals.
- **Síria:** El ciberespai, a Síria, està fortament regulat i controlat mitjançant noves legislacions que avalen pràctiques repressives per criminalitzar la llibertat d'expressió i el lliure flux d'informació. El govern utilitza diverses unitats del seu aparell de seguretat per monitorar comunicacions i regular l'accés a internet. Des de la Primavera Àrab, ha incrementat el seu control, amb la detenció d'activistes i la imposició de penes severes per difondre *fake news*. A més, es fan servir exèrcits electrònics i grups de hackers , per perseguir i vigilar opositores, tant dins com fora del país. La repressió és especialment intensa contra la població kurda, que veu com es violen el seu dret a reunió i la llibertat d'expressió.
- **Palestina:** L'ocupació israeliana de Gaza i Cisjordània ha permès l'experimentació i desenvolupament de tecnologies de vigilància, consolidant a Israel com a líder mundial en aquest àmbit. Aquesta col·laboració entre l'Estat i les empreses de ciberseguretat és cabdal per sostenir el sistema d'apartheid que pateix la població palestina. Les eines de repressió digital inclouen el monitoratge de les defensores de drets humans en xarxes socials i l'ús d'apagades d'internet com a càstig col·lectiu. El genocidi actual a Gaza ha intensificat aquestes violacions de drets, amb la introducció de la intel·ligència artificial per augmentar la letalitat dels atacs. A través de tecnologies avançades, com ara sistemes de reconeixement facial i armes autònomes, Israel ha incrementat el seu control i vigilància sobre les palestines, fet que ha exacerbat la crisi humanitària i la repressió a la regió.

- **Jordània:** La censura digital a Jordània ha augmentat significativament els últims anys i afecta principalment activistes LGBTIQ+ i periodistes. El govern utilitza la Llei de Ciberdelinqüència per intimidar i perseguir periodistes, la qual cosa ha portat al tancament de nombrosos llocs web independents. Concretament, durant les recents manifestacions a la capital jordana, que es van intensificar després del genocidi a Gaza, s'han instal·lat milers de càmeres de vigilància per a controlar i documentar les protestes i identificar-ne les participants.
- **L'Iraq:** La censura de contingut digital i l'assetjament en línia perpetrats per exèrcits electrònics a l'Iraq afecten greument a les dones i a la comunitat LGBTIQ+. Aquests atacs en línia sovint precedeixen a atacs físics. L'Iraq lidera l'ús de les apagades digitals a la regió, que s'apliquen especialment durant les mobilitzacions i protestes socials. Des de 2019, el govern ha bloquejat l'accés a internet en 126 ocasions, fet que ha contribuït a la violència contra activistes, perquè resulta més difícil informar sobre els abusos.

Les principals tendències de vigilància massiva identificades a la regió són:

1. **Augment de l'autoritarisme i la repressió de les dissidències:** Els governs de la regió han expandit les seves capacitats de control sobre la societat civil i han limitat el flux d'informació i la capacitat de mobilització dels moviments socials. Des de les Primaveres Àrabs, aquest procés s'ha reforçat mitjançant l'ús de tecnologies que permeten el monitoratge de la població i el control de les comunicacions.
2. **Participació d'empreses internacionals en el desenvolupament de tecnologies repressives:** Algunes empreses d'Israel, els Estats Units i d'Europa han subministrat tecnologies de vigilància i control que els governs de la regió utilitzen per a reprimir a les dissidències i espiar a les defensores de drets humans i periodistes. Aquesta repressió és més greu en els territoris ocupats.
3. **Ús de programari espia i ciberespionatge:** En països com el Marroc i Egipte, l'ús de programari espia com Pegasus permet vigilar dispositius de persones i organitzacions crítiques amb el règim. Aquestes tecnologies possibiliten l'assetjament digital i la recol·lecció d'informació privada per atacar la reputació d'activistes, periodistes i defensores de drets humans, i limita l'espai per a l'activisme i la llibertat d'expressió.
4. **Estratègies de control en les xarxes socials:** Per a controlar l'opinió pública, es realitzen campanyes de desinformació i manipulació a les xarxes socials, mitjançant comptes falsos que difonen contingut afí al règim i difamen les figures de l'oposició. En el cas de la població LGBTIQ+ i les dones defensores, s'ha detectat un assetjament diferencial que sovint usa informació privada per a difamar i desacreditar-les. En alguns contextos com l'Iraq i el Marroc, s'ha identificat com aquestes estratègies busquen fer còmplice la població en general, que trasllada l'assetjament iniciat a les xarxes també a l'espai públic.
5. **Apagades d'internet:** Davant del potencial organitzatiu de les noves tecnologies de la informació i les xarxes socials, s'ha identificat l'estratègia de "desconnexió"

per prevenir l'organització i les accions de denúncia dels moviments socials. S'ha observat que durant aquests bloquejos augmenta la repressió policial. A l'Iraq, a Palestina i a Síria aquesta pràctica és freqüent.

Conclusions clau:

1. **Erosió de l'espai cívic:** La vigilància massiva a la regió mediterrània limita significativament la llibertat d'expressió, la capacitat d'organització i la defensa dels drets humans, perquè crea un clima de repressió que provoca efectes diversos com l'autocensura.
2. **Complicitat internacional:** Els governs del Nord Global i les empreses d'aquests països han contribuït a desenvolupar i exportar tecnologies de vigilància sense mecanismes efectius de rendició de comptes, això perpetua la impunitat en les violacions dels drets humans.
3. **Afectació diferencial a col·lectius vulnerabilitzats:** Les dones, la comunitat LGBTIQ+, les persones migrants i les defensores de drets humans són les més afectades, no només per la vigilància, sinó també per l'assetjament digital i les amenaces específiques.
4. **El rol de l'ocupació en l'ecosistema de la vigilància massiva:** Gran part de les tecnologies identificades es desenvolupen i es posen a prova sobre el poble palestí que viu sota ocupació militar israeliana. Mentrestant, el Marroc s'ha convertit en un actor clau en el desenvolupament del sector a la regió, afectant greument els drets del poble sahrauí. Les ocupacions i el genocidi són factors que beneficien l'ecosistema empresarial de la vigilància.
5. **Necessitat urgent de regulació:** La falta de normatives específiques i de marcs legals que regulin l'ús de la vigilància massiva permet als governs abusar d'aquestes tecnologies en nom de la seguretat nacional i la lluita antiterrorista. Els mecanismes de protecció són ineficaços i això dificulta que les víctimes d'aquesta vigilància trobin justícia i reparació.

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