MASS SURVEILLANCE IN THE MAGHREB AND MASHREQ

A critical analysis to protect civil society

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

MASS SURVEILLANCE IN THE MAGHREB AND MASHREQ

A critical analysis to protect civil society

November 2024

Main authors: Dúnia Camps-Febrer, Felip Daza, Carlos Díaz and Nora Miralles

Contributing authors: Berta Flores and Paula Mas

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

Communication: Lucrecia Baquero Ramos (Observatorio de Derechos Humanos and Empresas en el Mediterráneo), Julia Ponti Estremens (NOVACT), Ionan Areses (SUDS)

Legal assistance: Laia Serra Perelló

Design: Carmela Márquez B @edicionescaseras

Translation: Lia Giralt

The Observatory on Human Rights and Business in the Mediterranean (ODHE) is a joint initiative of NOVACT and SUDS.

We are grateful to several people who have generously offered their help: Itxaso Domínguez de Olazábal, Ahmed Ali, and Omar Alaameri, Anabel Karina Arias, as well as to all the human rights defenders who have contributed to the research and to the entire SUDS and NOVACT team.

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

Report carried out in the framework of the project:
Alhimaya - Defending civic space and protecting human rights defenders in the Euro-Mediterranean.

With the support of:

Agència Catalana de Cooperació al Desenvolupament · Generalitat de Catalunya

INDEX

CLARIFICATIONS ON THE TERMINOLOGY USED:

International law considers the Palestinian territory of the West Bank, including East Jerusalem, and the Gaza Strip to be illegally occupied by Israel. Some authors argue that all historic Palestine—the area colonized under the British Mandate from 1918 to 1948—is occupied territory, given that the State of Israel was established through the expulsion of a large part of the Indigenous population, the Palestinian people. In this report, when we refer to the Occupied Palestinian Territory (OPT), we mean the Gaza Strip and/or the West Bank, including East Jerusalem.

The United Nations considers Western Sahara a non-self-governing territory whose decolonisation process is subject to the referendum on self-determination provided for in the 1991 Peace Plan. In this context, Spain is the administering power, while Morocco is considered the occupying power. For the African Union and more than 50 other states, Western Sahara is the Sahrawi Arab Democratic Republic, a sovereign state. In this report, when we speak of the occupied territory of Western Sahara, we refer to the Sahrawi Arab Democratic Republic.

Furthermore, in this report, we will use the generic feminine as a linguistic expression referring to persons.

FOREWORD

The indiscriminate use of mass surveillance by states and corporations is endangering the foundations of democracies globally.

New technologies are providing governments with increasingly powerful tools to control social movements, media and dissent in general. Technology and the surveillance trade operate virtually unregulated, becoming vital to this repressive architecture. This has led to the normalisation of illegal practices by some states, which use these tools to perpetuate control and repression. In this context, artificial intelligence has burst in, further elevating the dynamics of discrimination. Moreover, the existing regulations lack an extraterritorial focus and, with national security as a pretext, tend to incorporate exceptions. In September 2021, the United Nations High Commissioner for Human Rights called for an "urgent moratorium on the sale and use of artificial intelligence" and associated technologies, and according to the UN Rapporteur on Freedom of Expression, the implementation of surveillance and control mechanisms is affecting the right to freedom of expression, opinion and privacy with profound violations against human rights defenders and journalists.

Surveillance and monitoring mechanisms severely erode fundamental rights such as freedom of expression, opinion and privacy, with a particularly harsh impact on human rights defenders and journalists, who are often directly targeted by these harassment practices.

This report is a follow-up to our study "Mass Surveillance and the Control of Dissent in Europe" (2021), where we warned about European governments' use of these technologies. We now turn our attention to the Maghreb and Mashreq, two regions where there is a clear pattern: companies from the global North —mostly European, American and Israeli— develop technology that is often "battle-tested" in contexts of serious human rights violations, especially in occupied territories. Increasingly, authoritarian regimes subsequently acquire this technology to repress dissent and social movements. Thus, the rise of authoritarianism is underpinned by a web of organisations, companies and institutions that legitimise a social order of oppression based on the abuse of state and corporate power, social polarisation and the use of violence in its various forms.

From Morocco to Iraq, governments and private companies in the region are deploying increasingly sophisticated digital surveillance tools to identify, monitor and silence dissidents, journalists, human rights defenders, and feminist and environmental activists. Many of these governments are supported by the West, which endorses these repressive practices to quell any threat to the status quo. There is thus an interdependence in the development and use of surveillance technologies sustained in a global context of corporate impunity, which this report aims to make visible to identify and understand the trends that authoritarianism puts into practice worldwide, as well as its specificities on a local level.

The Mediterranean region is currently experiencing a severe limitation of civic space, which is indispensable for the exercise and defence of fundamental rights such as freedom of expression, association and assembly. These rights are crucial to ensure free and safe interaction between civil society and governments without fear of reprisals. Seeing how technology is creating the capabilities to keep dissent under control, we are concerned about the future of democracies. The rights achieved throughout history have not been granted but won through social struggles. It is of great concern that states increasingly have the tools to monitor, persecute and silence social and rights movements, thus putting many of our hard-won rights at risk.

This democratic degradation restricts civil society's capacity for self-organisation, involvement in public life, and defending human rights, with a severe impact on those groups most vulnerable to systems of oppression based on racism and gender and class categories.

In this context, we express our concern about how new technologies reinforce these inequalities, facilitating the systematic violation of rights and silencing any dissidents fighting against this authoritarian drift.

In this report, we provide analysis and diagnosis of what is happening, knowledge of the phenomenon and the nuances that occur in different contexts to build collective strategies to reverse it. We also provide arguments and tools to underline the urgent need to regulate these technologies, which not only weaken democracies but also endanger the lives of people and collectives working to defend them. The lack of international regulatory mechanisms makes it difficult for victims of targeted surveillance to find justice, redress and guarantees of non-repetition. Creating control and regulation systems is essential at both state and supra-state levels, both for the companies developing these technologies and those implementing and purchasing them. In this sense, we want to alert administrations to the urgent need to establish control and monitoring mechanisms to prevent the public contracting of companies and the purchase of technology linked to the violation of human rights throughout the supply chain. It is urgent to remind states and companies that it is their responsibility to ensure respect for human rights, and this report is a further step in that direction.

We do not want to end without mentioning the importance of creating north-south human rights advocacy networks and strategies that broaden local perspectives in an international exchange based on reciprocity. Interconnection, the exchange of experiences and the creation of alliances drive change and transformation for the entities that promote this research.

INTRODUCTION

Surveillance and control technologies, understood as the hardware and software needed to monitor the population's behaviour, activities and information, have become a lucrative business that, in 2022, already had a turnover of more than $130 billion and is estimated to exceed $150 billion globally[1]. This market is controlled primarily by Western companies, mainly Israeli, Central European, and American, whose products and technologies are being applied, as this report shows, in a profuse and increasingly widespread manner in the countries of the Global South.

This multi-million-dollar development and investment in artificial intelligence and digital technologies applied to social control occurs in a global context of rising authoritarianism, militarism and human rights violations —amid a worldwide ecological and economic crisis of uncertain consequences. Most human rights and democracy organisations worldwide share this perspective. Amnesty International warned in 2019 that "this global authoritarian drift is existential, threatening every human being and all our freedoms, equality and justice"[2].

However, the use of and access to digital technologies are also differentiated according to the characteristics of the population, highlighting aspects such as age, gender, or the urban-rural divide[3]. All these factors determine the impact of digital technologies, both as a means of accessing or producing diverse information and as a means of control and repression.

In the case of the Mediterranean region and, within it, the Maghreb and Mashreq, since the Arab Spring, regimes have invested in mass surveillance technologies to control political dissent. However, the most extreme case is Israel's use of the Occupied Palestinian Territory (OPT) as a laboratory for testing new weapons and technologies on the civilian population, which has allowed it to become a world leader in exporting technologies of repression and social control. This dynamic has been dramatically exacerbated since 7 October 2023. Since the beginning of the genocide in Gaza, more than 41,000 Palestinians have been killed by the Israeli army, in a context where extremely lethal artificial intelligence systems have been deployed.

These attacks in Gaza have enhanced the use and abuse of surveillance not only against the Palestinian population in the OPT but also against the civil society that has risen around the world to denounce the massacres and the inaction of the international community. Added to this is the forced digital disconnection of the Lebanese population in villages and suburbs

---

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

3 See data by country: **Arab Barometer.** "The MENA Digital Divide." Available at: https://www.arabbarometer.org/2020/09/the-mena-digital-divide/.

whose communications infrastructure has recently been bombed and destroyed by Israel. Intimidating messages and false calls for evacuation through networks and messaging apps to confuse, intimidate and frighten the Lebanese population have also been documented in the targeted areas. These trends undoubtedly hint at yet another turn of the screw in the global authoritarian drift and deserve their urgent analysis[4].

This report analyses the trends and direction that mass surveillance in the Maghreb and Mashreq has taken in recent years, in continuity with the research project "Hi-tech surveillance in times of COVID-19"[5] published by ODHE in 2021, in which some of these trends and companies were already featured. We aim to facilitate an understanding of how, in the deployment of their internal security policies, the relationship between governments and the tech business sector impacts human rights abuses. The research on cases and products has been complemented by interviews with human rights defenders who, in some cases, participated in the meeting "The Nonviolence Factory", organised by NOVACT, held in November 2023 in Barcelona, as well as in the "Al-Himaya Seminar on defence and protection of civic space against mass surveillance in the Euro-Mediterranean", organised by SUDS, NOVACT and Irídia, in May 2024.

To this end, it is essential to understand how these technologies have been developed and tested and the social and political implications of using these tools from a human rights perspective. An intersectional approach to unmasking the global chain of repression and social control can strengthen the protection, mobilisation, communication, and advocacy work of groups and collectives affected by these violations and establish alliances between human rights defenders from different territories.

Aware that our position and tools are in Barcelona, we have adopted a decolonial, anti-racist and feminist perspective. For this reason, the methodology incorporates the knowledge and experience of the organisations and human rights defenders we have interviewed in various Mashreq and Maghreb countries.

There is a technological interdependence in which the global north extracts raw materials from countries in the global south to manufacture technologies that are tested on the populations of these countries and then used to hone surveillance on human rights defenders, journalists, political opposition, gender and sexual dissidents or migrants around the world.

This context obliges us to identify and understand the implications of mass surveillance on human rights and human rights defenders across the Mediterranean region and to assume our responsibility as a part of the global North.

---

4 **SMEX.** "Digital Rights During the War on Lebanon". 10 October 2024. Available at: https://smex.org/digital-rights-during-the-war-on-lebanon-october-9-2024/.

5 **ODHE.** "Mass Surveillance." Available at: https://mass-surveillance.odhe.cat/.

I

MOROCCO: THE ALAWITE PANOPTICON

Digital surveillance in Morocco mainly targets independent journalists, human rights defenders and the Sahrawi population (see the chapter on Western Sahara). The repression of visible dissidents is a very effective strategy, as it reinforces the feeling of total control over the rest of the population, which resorts to self-censorship to avoid repression. Morocco also monitors persons of interest outside the country (from presidents and heads of state to foreign journalists). Apparent arbitrariness has always been part of the regime's repressive strategy. On the one hand, the persecution of high-profile figures ensures that no high profile is protected. On the other, the repression of the anonymous population propagates the idea of total control: the Alawite panopticon[6] .

"The repression of visible dissidents is a very effective strategy, as it reinforces the feeling of total control over the rest of the population, which resorts to self-censorship to avoid repression"

The Casablanca bombings of May 2003 accelerated Morocco's entry into the US-promoted counter-terrorism framework[7]. The 2003 anti-terrorism law, controversial but passed unanimously in the aftermath of the attacks, gave a free hand to monitor the media and the content of websites, blogs and other spaces. Thousands of people were arrested and detained without charge for days,[8] and organisations, movements and human rights defenders critical of the regime were monitored under the excuse of 'national security' and 'public order'[9].

Since the early 2000s, Morocco has been adopting laws to control the digital world (Cybercrime Law in 2003, Cybersecurity Law in 2020)[10]. In September 2011, the General

6 The first known arrest for personal online content was in February 2008. The arrest by plainclothes officers of Fouad Mourtada for creating a fake profile of the king's brother uncovered possible mass online surveillance. Fouad was not a known activist.

7 Collaboration with the United States in its "War on Terror" had already begun before 2003. Morocco was one of the countries that contributed black sites (the name given to clandestine detention centres operated by the CIA, generally located outside the continental United States and its jurisdiction) for the kidnapping and torture of CIA prisoners after the 2001 attacks. **Tom Finn.** "How Arab states helped the CIA with its torture-linked rendition program." Middle East Eye, 13 February 2015.
Available at:
https://www.middleeasteye.net/news/how-arab-states-helped-cia-its-torture-linked-rendition-program.

8 The 2003 anti-terrorism law also allows a person to be detained for up to 12 days without tr. **Human Rights Watch**. "Stop Looking for Your Son. Illegal Detentions under the Counterterrorism Law." 25 October 2010.
Available at:
https://www.hrw.org/report/2010/10/25/morocco-stop-looking-your-son/illegal-detentions-under-counterterrorism-law.

9 In addition, crimes of opinion against the monarchy, religion and 'national sovereignty' can lead to up to six years in prison. **Departamento de Estado, EUA**. "Morocco 2023 Human Rights Report."
Available at:
https://www.state.gov/wp-content/uploads/2024/02/528267_MOROCCO-2023-HUMAN-RIGHTS-REPORT.pdf.

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

Directory of Information Systems Security[11] and maCERT, the "Centre for Monitoring, Detecting and Responding to Cyber-attacks", were created. Both the Directorate and maCERT are under the direction of the National Defence Administration[12], which is equivalent to the Ministry of Defence. This means that part of the monitoring infrastructure has been created not under the umbrella of the Ministry of Interior or Information but within a military institution in which accountability and transparency are absent[13].

Although, according to *Freedom House,* Morocco is 'partly free'[14] in internet access and freedoms, adopting press laws and freedoms with acceptable standards hides the pernicious use of the judicial system and the penal code[15]. Most human rights defenders and journalists have not been charged and convicted under the Press and Publications Law but under crimes defined in the Penal Code and carrying prison sentences. This combines repressive legislation, the necessary connivance of the judicial system, and a network of intrusive technologies, many of them which are developed by European companies.

11 The Directorate of Information Systems Security was created by Decree N° 2-11-509 of 21 September 2011. It is an administration attached to the National Defence Administration.

12 Hassan II abolished the Ministry of Defence in 1972. Currently the National Defence Administration reports directly to the King through the Deputy Minister of the ADN, also Minister of the Interior, Abdellatif Loudiyi.

13 **Freedom House**, "Freedom on the Net 2023: Morocco," accessed 12 September 2024. Available at: https://freedomhouse.org/country/morocco/freedom-net/2023.

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

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

1. SOCIAL NETWORKS, MOBILISATION AND FEAR OF LOSING CONTROL OF THE NARRATIVE

The increased use of social media began to pose a problem for the regime in 2007 with cases such as the Targuist sniper[16] [17], when the population denounced the system on its own. However, the most significant turning point in digital surveillance was during the 2011 uprisings and the 20 February Movement[18]. The great mobilising power of civil society in the 2011 uprisings that spread across the region was carried out through the internet, mainly via Facebook and YouTube, such as the *Mamfakinch*, campaign, organised by a social collective days before the first protests in February[19] [20].

One of the first known Moroccan purchases for digital control was Hacking Team's malware[21] the Italian tech company's remotely triggered Trojan[22] It was used against journalists and the *Mamfakinch* campaign[23]. Two Moroccan intelligence agencies (Conseil Supérieur de la Défense Nationale—CSDN and Direction Générale de Surveillance Territoriale—DST) were among the clients who bought it in 2009 and 2012, respectively[24].

16 **Jeune Afrique**, "Corruption au Maroc : le " sniper de Targuist " poursuit son combat à visage découvert," 4 March 2013. Available at: 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." Available at: https://www.youtube.com/watch?v=l9lVKf5Hk4Q.

18 Mass movement whose political demands included reforming the country's political system.

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

20 Despite the repression, several mobilisation campaigns on the internet had a great impact, such as the September 2018 #Masaktach ('I will not shut up') campaign against male violence and sexual harassment; or the boycott campaign the same year against several companies closely linked to the regime (Central Danone, Sidi Ali, Afriquia). **Freedom House**. *Freedom on the Net 2019*. Available at: https://freedomhouse.org/country/morocco/.

21 See glossary.

22 See glossary.

23 **Privacy International.** *Their Eyes on Me: Stories of Surveillance in Morocco*. 7 April 2015. Available at: https://privacyinternational.org/report/1125/their-eyes-me-stories-surveillance-morocco.

24 Ibid.

In October 2016, the massive HIraq Rif (Popular Rif Movement) protests erupted, gathering thousands of people for weeks in Al Hoceima and other towns in northern Morocco. In addition to repression on the ground, human rights defenders, journalists and bloggers were arrested between May and August 2017 for their activities on the internet[25] [26].

2. MANIPULATING SOCIAL NETWORKS

Currently, social networks are the primary source of information for the Moroccan population, with YouTube and Facebook leading the way[27], They are the only forms of communication that go beyond the official discourse. Therefore, these networks are the focus of control and repression, which is carried out with different strategies.

One of these has been the use of networks of coordinated inauthentic behaviour[28] that seek to influence public opinion locally and regionally. Meta deleted hundreds of Facebook and Instagram accounts linked to pro-government activities, praising the Moroccan Government's handling of the pandemic, its diplomatic initiatives and the security forces' response, and praising King Mohammed VI and senior security officials[29] [30]. The accounts were linked to pro-regime media such as ChoufTV, known for its defamatory work against human rights defenders[31]. Meta says some 150,000 accounts followed one or more of these sites.

25 Peaceful activists such as Nasser Zefzafi and El Mortada Iamrachen were charged with 'breaking respect for the king', 'offending constitutional institutions' or 'insulting public officials'. Rabieh Al-Ablaq was sentenced in June 2017 to 5 years in prison for 'publishing false news' and 'usurping the title of journalist'. Al-Ablaq denounced the torture he suffered during police interrogations in Alhuceimas.

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

27 There are, however, substantial differences in internet access and use between men and women, between rural and urban populations, and between young people and people over 30. **Arab Barometer**, 'The MENA Digital Divide,' September 2020.
Available at: https://www.arabbarometer.org/2020/09/the-mena-digital-divide/.

28 See glossary.

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

30 In February 2021 alone, 385 Facebook accounts and 6 Facebook pages, as well as 40 Instagram accounts operated from Morocco and targeting the public, were deleted in Morocco. This network of accounts was dismantled by Meta following Amnesty International›s complaints. **Facebook**, "February 2021 CIB Report,". March 2021.
Available at: https://about.fb.com/wp-content/uploads/2021/03/February-2021-CIB-Report.pdf.

31 **DNA**, "Defamation Campaign against Human Rights Defender Karima Nadir," *Frontline Defenders*, accessed 12 September 2024.
Available at: https://www.frontlinedefenders.org/en/case/defamation-campaign-against-woman-human-rights-defender-karima-nadir.

3. MASS SURVEILLANCE AND MONITORING OF COMMUNICATIONS

State-of-the-art technologies support mass surveillance and control of communications. This involves monitoring the information circulating and published and occasional digital blackouts[32]. Although filtering (blocking of specific sites and data) is not one of the most widely used tools, it is still used arbitrarily and without official warning[33]. These particularly intrusive surveillance mechanisms target human rights defenders and regime critics.

In 2019, Amnesty International reported that the devices of prominent human rights defenders had been infected by Pegasus. Among them, Sahrawi human rights defender Aminatou Haidar, historian Maati Monjib; journalists and researchers Taoufik Bouachrine, Omar Radi, Soulaimane Raissouni; and human rights lawyer Abdessadak El Bouchattaoui. According to these journalists, some of the content and materials obtained through Pegasus were used to defame, blackmail and harass them.

In 2022, Amnesty International and Citizen Lab found solid evidence of the Moroccan authorities using the spyware[34] Pegasus from Israel's NSO Group. A list was made of up to 10,000 people possibly affected, including King Mohammed VI himself[35] [36]. Morocco also spied on Sahrawi human rights defenders and prominent figures abroad, including French journalists and President Emmanuel Macron, Spanish Prime Minister Pedro Sánchez and the Ministers of Defence, Interior and Agriculture. Although NSO has not denied using its software in these cases, it has not published the results of an investigation it promised to carry out in 2019. In addition, the Moroccan Interior Ministry has reportedly been a client[37] of Circles Technologies since at least 2018, using a system from this NSO Group-affiliated company to monitor calls, text messages and locations based on network vulnerabilities.

---

32 From 25 to 30 May 2007, YouTube was blocked by the largest EPS Maroc Telecom (the other two providers Wana and Meditel did not block it). Global Voices, 'Morocco Blocks Access to YouTube,'. 26 May 2007. Available at: https://globalvoices.org/2007/05/26/morocco-blocks-access-to-youtube/.

33 In January 2016, the three HPS blocked VoIP calls on 3G and 4G (Skype, Viber, Tango, WhatsApp and Facebook Messenger among others). Saad Guerraoui, 'Morocco banned Skype, Viber, WhatsApp and Facebook Messenger. It didn't go down well', *Middle East Eye*. 9 March 2016.
Available at:
https://www.middleeasteye.net/opinion/morocco-banned-skype-viber-whatsapp-and-facebook-messenger-it-didnt-go-down-well.

34 See glossary.

35 **Forbidden Stories.** "About the Pegasus Project." *Forbidden Stories*. 18 July 2021.
Available at: https://forbiddenstories.org/about-the-pegasus-project/.

36 **El País.** "Macron, in the crosshairs of the Pegasus spying programme contracted by Morocco." *El País*, 20 July 2021.
https://elpais.com/internacional/2021-07-20/macron-en-el-punto-de-mira-del-programa-de-espionaje-pegasus-contratado-por-marruecos.html.

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

On the other hand, the French investigative journalism group Reflet uncovered Morocco's purchase of the Eagle System[38]. owned by the French company Amesys (Nexa Technologies), for mass digital surveillance of internet traffic with censorship functions (through Deep Packet Inspection[39]), In 2011, Morocco invested around €2 million in the Eagle System, which was developed in Morocco under the name "Project Popcorn"[40].

Citizen Lab's investigation also uncovered Morocco's High Council of National Defence purchasing malware[41] known as FINFIsher[42] (or Finspy) from the Anglo-American company Gamma Group[43]. The software is sold exclusively to government agencies and police forces through Lench IT Solutions plc. It remotely controls any previously infected device and can copy files, intercept Skype calls, and even record keyboard movements.

38 **Privacy International**. *Their Eyes on Me: Stories of Surveillance in Morocco*, 2015.
Available at: https://privacyinternational.org/report/1125/their-eyes-me-stories-surveillance-morocco.

39 See glossary.

40 **Reflets.info**, "Maroc : Popcorn, le projet qui n'existait pas," 15 November 2017.
Available at: https://reflets.info/articles/maroc-popcorn-le-projet-qui-n-existait-pas.

41 See glossary.

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 October 2015.
Available at: 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 October 2015.
Available at:
https://www.zdnet.com/article/in-hacking-teams-wake-finfisher-spyware-rises-in-popularity-with-government-users/.

4. ONLINE HARASSMENT: SMEAR CAMPAIGNS AND DIGITAL AMBUSHES[44]

Online attacks and trolling[45] have included smear campaigns, a strategy widely used in Morocco. Human Rights Watch calls these "character assassination campaigns", in which, in an orchestrated manner, smear campaigns and hoaxes are launched[46]. Very often, these campaigns attack the sexual freedoms of human rights defenders. In a December 2021 Meta report[47], Morocco is identified as a source of Facebook and Instagram account profiles linked to the Israeli software Cognyte (formerly WebintPro). This software allows creating and managing fake accounts on social networks such as Facebook, Instagram, Twitter, and YouTube. It also collects data from these social networks. According to the same Meta report, it mainly targets journalists and politicians[48]. In addition, several hacker groups that act to sabotage critical content on the networks or infiltrate social networks or private emails have been identified[49].

"Defenders who are journalists or public figures critical of the government are primarily targeted with online sexist violence, with ongoing smear campaigns about their sexual freedom and harassment"

Defenders who are journalists or public figures critical of the government are primarily targeted with online sexist violence, with ongoing smear campaigns about their sexual freedom

44 See glossary.

45 See glossary.

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

47 **Mike Dvilyanski, David Agranovich and Nathaniel Gleicher**, "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 December 2021. Available at: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

48 **Mike Dvilyanski, David Agranovich and Nathaniel Gleicher**, "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 December 2021. Available at: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

49 In September 2013, the Investigative Journalism website in Morocco was hacked and its content replaced with porn (a common strategy). The independent news platform Lakome.com was blocked by the courts on 17 October 2013 and has not been reinstated. Its director and journalist, Ali Anouzla, was also detained under the Anti-Terrorism Law for linking to an article in the country about Al-Qaeda. **Reporters Without Borders**, "Website editor held for posting Al Qaeda video," 20 September 2013. Available at: https://web.archive.org/web/20150610182747/http://en.rsf.org/morocco-website-editor-held-for-posting-19-09-2013,45197.html.

and harassment[50]. ChoufTV, in 2020, published defamatory information about rights activist Karima Nadir[51].

Human Rights Watch also denounces digital entrapment attacks[52] against LGBTIQ+ people. In 2020, a homophobic campaign of forced outings[53] of gay or bisexual men was orchestrated through apps[54]. Same-sex relationships are forbidden in Morocco, and in addition to prosecution, such information can have serious social consequences for individuals, such as direct physical violence, professional reprisals, etc.

Online repression often has three consequences: self-censorship, sex-related exile[55] or physical repression. Following sexualised smear campaigns, journalist Taoufik Bouachrine, editor of the daily paper Akhbar al Yaum, was sentenced in 2018 to 15 years in prison for several crimes (human trafficking, sexual assault, rape, prostitution and harassment) after a hectic media campaign[56]. Her colleague Hajar Raissouni was arrested in 2019 on charges of "illegal abortion" and "sexual relations outside marriage" and for being pregnant by her boss[57]. The Moroccan authorities tried to prove the charges at all costs, including forcing her to undergo a medical examination without her consent. She was sentenced to one year in prison before being released by royal pardon[58] and forced to leave the country.

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

51 Calling for her arrest, accusing her of drug use and neglectful single parenting. Karima Nadir is co-founder of the 490 Collective and vice-president of the Digital Rights Association.

52 See glossary.

53 See glossary.

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

55 Refers to the situation where LGBTIQ+ people are forced to leave their place of origin due to discrimination, rejection or violence they face because of their sexual orientation or gender identity.

56 The Euro-Mediterranean Human Rights Monitor identified more than 30 pro-regime websites and online newspapers that had engaged in such campaigns. **Reporters Without Borders**, "After long jail term, Moroccan journalist hit by heavy damages award," 7 December 2018.
Available at: https://rsf.org/en/after-long-jail-term-moroccan-journalist-hit-heavy-damages-award.

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

58 The royal pardon is repeated on important national holidays. On these occasions, a list of 'pardons' that the king grants to persons previously convicted by the courts is published. The arbitrariness of the Royal Pardon is obvious. In 2020, the royal pardon included members of the Rif Movement. In 2024, several high-profile journalists were 'pardoned': Omar Radi, Souleimane Raissouni and Taoufik Bouachrine, Hicham Mansouri, Samad Ait Aicha, Imad Stitou, and Afaf Bernani.

II

WESTERN SAHARA: SURVEILLANCE TO MAINTAIN THE OCCUPATION

Since the breakdown of the 1991 truce between the Polisario Front and Morocco and following the raid by Moroccan forces on 13 November 2020 to expel a group of Sahrawi activists protesting the plunder of resources in Moroccan-occupied Western Sahara, hostilities between the two actors have intensified. At the same time, the repression and persecution of pro-Saharawi organisations and defenders has also increased.

1. MODERNISATION OF MOROCCO'S SURVEILLANCE SYSTEMS

Morocco's occupation of Western Sahara has depended, in large part, on the ability to control, monitor, and repress the Sahrawi population. Since 2020, the human rights situation in the occupied territory of Western Sahara has become more alarming. The increasing digitalisation of the African and Moroccan landscape has influenced the methods, impact, and increase of surveillance strategies for the population of Western Sahara[59]. Moreover, Morocco's rapprochement with Israel, since the re-establishment of relations in 2020[60], has enabled its collaboration in the modernisation and development of intelligence and surveillance tools. In parallel, since 2009, agreements have been reached with the Spanish company Indra Sistemas, S.A. Indra signed a 6.3-million-euro contract to install three stations extending its satellite surveillance network in El Aaiún, Smara and Dakhla[61]. In May 2024, Indra and the Moroccan Digital Development Agency (ADD) signed an agreement to accelerate Morocco's digital transformation process[62].

The surveillance of the Saharawi civilian population by the Moroccan authorities has been based on the use of their labour force, the introduction of informants and settlers, the control of borders, the isolation of the population and the persecution and repression of dissent[63]. The Moroccan authorities have been subjecting the Saharawi population to constant

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*. December 10, 2020.
Available at: 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 December 2020.
Available at: https://www.nytimes.com/2020/12/10/world/middleeast/israel-morocco-trump.html.

61 **Indra.** "Morocco to improve air traffic management with Indra's technology". 29 October 2009.
https://www.indracompany.com/es/noticia/marruecos-mejorara-gestion-trafico-aereo-tecnologia-indra.

62 **El Economista**. "Indra to drive Morocco's digital transformation." *El Economista*. 17 May 2024.
https://www.eleconomista.es/telecomunicaciones/noticias/12841197/05/24/indra-impulsara-la-transformacion-digital-de-marruecos.html.

63 **ECSaharawi**. "Morocco intensifies its spying in occupied Western Sahara for fear of popular uprising." 7 August 2024.
https://ecsaharaui.com/07/2024/marruecos-intensifica-su-espionaje-en-el-sahara-occidental-ocupado-por-temor-a-un-levantamiento-popular/.

surveillance, both physical and technological[64]; as reported by media such as Por Un Sahara Libre (PUSL)[65]. Other sources denounce the use of surveillance cameras in El Aaiún, Smara, Dakhla and even in smaller towns in Moroccan-occupied Western Sahara[66].

The two central bodies conducting this surveillance are the Moroccan police forces and the Directorate General of Territorial Surveillance (DGT in French), the governmental body of Morocco's civilian intelligence service. These two bodies of the Moroccan forces[67] are integrating new technologies into their strategies and control mechanisms. Since 2023, the DGT has been collaborating with the US Federal Bureau of Investigation (FBI) in an 'anti-terrorist' alliance that addresses the 'Sahara-Sahelian' zone[68] and ultimately facilitates control over dissidents in the territory.

64 **Amnesty International**, "Rights Trampled: Protests, Violence and Repression in Western Sahara," 2010. Available at: https://www.amnesty.org/es/wp-content/uploads/sites/4/2021/07/mde290192010es.pdf.

65 **For a Free Sahara.** *Official website on the situation in Western Sahara and the struggle for self-determination.* Retrieved from https://porunsaharalibre.org/.

66 **ECSaharawi**. "Western Sahara: Morocco spies with reconnaissance cameras on Saharawis in occupied El Ayoun." 7 August 2024.
https://ecsaharaui.com/07/2024/sahara-occidental-marruecos-espia-con-camaras-de-reconocimiento-a-los-saharauis-en-el-aaiun-ocupado/.

67 **Amnesty International**, "Rights Trampled: Protests, Violence and Repression in Western Sahara," 2010. Available at: https://www.amnesty.org/es/wp-content/uploads/sites/4/2021/07/mde290192010es.pdf.

68 **Swissinfo**, "FBI and Moroccan DGST expand counter-terrorism collaboration in the Sahel," 21 February 2023. Available at:
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: FROM INSTITUTIONAL SURVEILLANCE TO 'SELF-SURVEILLANCE'.

The Moroccan state declared a state of emergency on 20 March 2020 to protect the population from the COVID-19 pandemic[69]. On 23 March 2020, the state of emergency was approved with Law No. 2.20.292, which establishes penalties and fines for anyone failing to comply with "orders and decisions of the authorities" and for anyone who "obstructs" such decisions, including the dissemination of "writings, publications or photos" on social networks[70].

In terms of technology, one of the main initiatives was the development of a mobile application by engineers and technicians from the Moroccan Directorate General of National Security (DGSN) with the support of the Ministry of Health and the Ministry of Interior[71]. The application Wiqaytna is a voluntary tool to identify people who have been in contact with someone positive for COVID-19. The app complies with Law No. 09-08, Article 4, which does not oblige the authorities to obtain a person's consent to process their data when used to protect the public interest, allowing for mass monitoring of the population's movements[72].

The Moroccan authorities officially ended the state of health emergency in February 2023,[73] deactivating Law No. 2.20.292. Still, it can be seen how the strategy of self-surveillance and population censorship has been translated into other cyber-surveillance policies. In June 2024, the General Directorate of National Security launched the E-Blagh platform[74] that allows civil society to report cybercrimes and directly notify the authorities of any digital infraction or crime, which, according to article 267-591 of the Moroccan Penal Code, includes "any threat to the integrity of the Kingdom of

69 **Europa Press Internacional**, "Morocco declares state of emergency from this Friday and 'until further notice' over coronavirus," 20 March 2020.
Available at:
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," submitted to the Parliament of the Kingdom of Morocco, 2020.
Available at: https://www.cg.gov.ma/fr/node/9696.

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

Morocco". The development of this platform involves the population in reporting and monitoring cybercrime[75].

3. MEDIA CONTROL AND PERSECUTION OF JOURNALISTS

Control of the media and censorship of journalism have been vital strategies of the Moroccan Government to maintain control over Western Sahara and defend its legitimacy internationally[76]. According to a Reporters Without Borders report on violations against the journalistic sector in this conflict, "journalism is one of the many victims of this media-neglected conflict, which has turned Western Sahara into a real information 'hole'"[77]. Digital development has affected Sahrawi journalists, with persecution using digital media. In the words of journalist Ahmed Ettanji of Equipe Media, "Digital repression is also a critical issue because most of our work is digital; it is based on social networks and more on alternative media"[78]. According to Ettanji, this has an "individual impact in limiting movement, because you are under surveillance. Whether physically or technologically" preventing one from working "freely"[79].

Moreover, journalists suffer from a double vulnerability, as in the case of Nazha el Khalidi, who was interrogated and tortured by Moroccan police forces and suffered sexist defamation[80].In the same vein, according to the 2007 OpenNet Initiative report[81], Morocco has censored numerous websites, mainly those supporting the independence of Western Sahara, such as the website of the Union of Sahrawi Journalists and Writers[82].

75 **MAP Express**."DGSN launches new 'E-Blagh' platform dedicated to fighting cybercrime." 6 June 2024. https://www.mapexpress.ma/actualite/societe-et-regions/dgsn-lance-nouvelle-plateforme-e-blagh-dediee-lutte-contre-cybercriminalite/.

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

77 **Reporters Without Borders**, "Morocco/Western Sahara," *Reporters Without Borders*. Available at: https://rsf.org/es/pais/marruecos-sahara-occidental.

78 Ahmed Ettanji, interview conducted as part of The Nonviolence Factory, November 2023. NOVACT team, SUDS, IRIDIA and ODHE.

79 Ibid

80 **Reporters Without Borders,** "Western Sahara, a desert for journalism," 2019. Available at: https://www.rsf-es.org/wp-content/uploads/attachments/2019_SAHARA_OCCIDENTAL_RSF_ES_INFORME.pdf.

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

82 **Union of Saharawi Journalists and Writers (UPES)**, "UPES". Available at: www.upes.org

As a tool of persecution and control of journalists, the Moroccan Government mainly uses the spyware[83] espía Pegasus, perteneciente al grupo israelí NSO Group. Según Amnesty International, Pegasus, belonging to the Israeli NSO Group. According to Amnesty International, this technology has also been used to spy on Sahrawi human rights defenders[84], including human rights defender Aminatou Haidar[85]. Amnesty International blames the lack of transparency in the surveillance industry (by companies and governments) for making it difficult to know which tools are being used, sold and bought, thus preventing victims from seeking accountability.

Spywares[86] are frequently used to identify dissident journalists and silence their work. In addition, the increased persecution of Sahrawi journalists has made it more challenging to document human rights violations in Western Sahara from outside the territory. A paradigmatic case of harassment was the repression of Equipe Media's Sahrawi human rights defender couple, Ahmed Ettanji and Naziha El Khalidi, who were placed under house arrest and even had their wedding prevented. The attacks on Saharawi journalists are believed to be a direct response to their reporting on the ongoing repression in the occupied territory. This activity puts their physical integrity at risk[87]. The persecution of Saharawi journalists limits their freedom of movement and prevents them from carrying out their work freely. Persecution also affects the family environment and the mental health of journalists, generating an economic impact and deteriorating social cohesion. In addition, the gender factor has aggravated the vulnerability of journalists, exposing them to more significant risks and reprisals, as documented in the cases of violence,

"lack of transparency in the surveillance industry (by companies and governments) for making it difficult to know which tools are being used, sold and bought, thus preventing victims from seeking accountability"

83 See glossary.

84 **Amnesty International**,"Morocco/Western Sahara: Activist Targeted with Pegasus Spyware in Recent Months - New Evidence," 22 October 2023.
Available at:
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 March 2022.
Available at:
https://www.middleeasteye.net/news/pegasus-spyware-morocco-western-sahara-activist-targeted

86 See glossary.

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

for example, suffered by Sahrawi human rights defenders Mbarka Mohamed al-Hafiz and Fatima Mohamed al-Hafiz[88].

4. USING DRONES TO CONTROL AND ATTACK FROM THE AIR

Following the end of the 2020 ceasefire, which exacerbated hostilities, Morocco has been using drone technology to establish its control over Western Sahara, both to carry out attacks and to monitor activities in the occupied territory and refugee camps[89]. Drone attacks are allegedly targeted at Polisario Front fighters. Still, their use has affected civilians from a variety of backgrounds, exacerbating the escalation of the conflict beyond the territory of Western Sahara[90]. For example, a Moroccan drone strike in 2021 in Polisario-controlled Western Sahara killed three Algerian truck drivers[91]. According to *Africa Intelligence*[92], since 2020, the Moroccan Government has integrated drone technology to monitor the Sahrawi camps and its borders with Algeria. Since the escalation of the conflict in 2021, the Moroccan Government signed a contract with the Turkish company Baykar to purchase Bayraktar TB2 drones[93] specialised in surveillance and reconnaissance[94]. Some websites mention that since 2023, Morocco has acquired armed

88 **Middle East Eye**, "Western Sahara Female Activists Face Rape, Divorce, and House Arrest," 21 April 2022. Available at: 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 May 2023. Available at: 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 May 2024. Available at: https://www.lemonde.fr/en/le-monde-africa/article/2024/05/09/morocco-to-become-rare-military-drone-manufacturer-thanks-to-cooperation-with-israel_6670920_124.html#:~:text=Israeli%20company%20BlueBird%20Aero%20Systems,a%20production%20facility%20in%20Rabat.&text=Joining%20South%20Africa%2C%20Egypt%20and,countries%20that%20build%20military%20drones.

91 **Menadefense**, "Comprendre l'attaque marocaine contre les civils algériens," accessed 10 September 2024. Available at: 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 December 2021. Available at: 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.

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

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

Akinci drones[95], which have been recorded flying over Smara territory in occupied Western Sahara[96]. The annual report of the Sahrawi Mine Action Coordination Office (SMACO) highlights 73 Moroccan drone attacks against civilians between 2021 and 2023, resulting in 160 civilian casualties, including 80 deaths[97]. The indiscriminate nature of these attacks has caused severe injuries and fatalities among Sahrawi, Mauritanian and Algerian civilian populations[98].

The development of drone technology and the end of the ceasefire have been accompanied by the development of the Moroccan Structural Law No. 10.20[99], which, through its 55 articles, allows and encourages the construction of units for the arms industry in Morocco, the manufacture of weapons through national operators, as well as encouraging foreign investment in this sector[100]. At the same time, the normalisation of relations between Morocco and Israel in 2020[101] has fostered military cooperation between these two actors, leading to a memorandum of understanding in 2021 between the two countries in the field of defence[102]. Following this agreement, the Israeli company Blue Bird Aero Systems plans to establish a drone production plant for Morocco's WanderB and ThunderB models, mainly for reconnaissance, intelligence, and target detection mis-

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

96 **Morocco Mail**. "Le drone Bayraktar TB-2 opérationnel au Sahara Occidental: Maroc-Algerie."
Available at:
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 May 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.
Available at:
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 July 2020.
Available at:
https://www.moroccoworldnews.com/2020/07/310459/new-framework-law-sets-ground-for-arms-industry-in-morocco.

101 **Juan José Vagni and Ignacio Rivas.** "Morocco and the Normalisation of Relations with Israel: Foundations and Projection of a Singular Approach," in *And Now Where Do We Go: New Challenges in the Middle East*, ed. Juan José Vagni and Ignacio Rivas. 2023.
Available at: https://sedici.unlp.edu.ar/handle/10915/162819.

102 **Government of Israel.** "Israel and Morocco sign historic Memorandum of Understanding on Defence." November 24, 2021.
Available at:
https://www.gov.il/en/pages/israel-and-morocco-sign-historic-defense-mou-24-november-2021.

sions[103]. These drone attacks are displacing the Sahrawi population outside their territory, violating their rights to housing[104], their right to free movement, cultural identity, and the right to protection against arbitrary displacement[105].

103 **Diaride Girona.** "Israeli company to open drone factory in Morocco". 28 April 2024. Available at: https://www.diaridegirona.cat/economia/2024/04/28/empresa-israeli-abrira-fabrica-drones-101651241.html.

104 **United Nations**. Universal Declaration of Human Rights, 10 December 1948. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

105 **The Guiding Principles on Internal Displacement.** United Nations, 1998. Available at: https://www.internal-displacement.org/sites/default/files/publications/documents/1998_Guiding_Principles.pdf.

III

TUNISIA: A PERMANENT STATE OF EMERGENCY

During the two decades that Tunisia was ruled by the autocrat Zine el Abidine Ben Ali, who was overthrown in 2011, the government extended its surveillance to the private spaces of the population through a particularly invasive security apparatus. After the fall of the regime following the 2011 Jasmine Revolution, the situation seemed to reverse, and the use of technology to hold power accountable grew, for example, by taking cameras to demonstrations and protests to record police abuses[106]. Then, the cyber-surveillance mechanism with which Ben Ali's Government had been censoring blogs and media critical of power (via the Tunisian Internet Agency) came to light. Known as Ammar 404[107], it became the symbol of mass surveillance during the dictatorship.

Almost fifteen years later, Tunisia is today a country in a permanent state of emergency, partially reusing the legal and technological architecture of the dictatorship to monitor and repress judges, journalists, lawyers, trade unionists, political opposition and LGBTIQ+ activists through anti-terrorism and cybercrime laws[108]. While Tunisia has remained in Freedom House's Freedom of the Press Index as the most compliant Arab country, the organisation acknowledges in its 2023 annual report that Tunisians are persecuted for posting content critical of the president, the government or the security forces[109].

1. RECOVERING THE DIGITAL SURVEILLANCE STRUCTURES OF THE DICTATORSHIP

During the last years of Ben Ali's regime, two parallel trends coexisted: the increase in internet access for the Tunisian population and the tight control of communications, symbolised by Ammar 404. This error message appeared when trying to access one of the numerous censored websites from inside the country, including Al Jazeera, Al Arabiya and critical Tunisian digital media such as Nawaat[110] [111]. This system monitored bloggers and journalists who were critical of the authorities. Political dissidents' emails were

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

107 **Webdo TN**. "Tunisie: Qui se cachait derrière Ammar 404 ?" 31 January 2011.
Available at: https://www.webdo.tn/fr/actualite/national/qui-se-cachait-derriere-ammar-404/173718.

108 **Amnesty International.** "Tunisia." Accessed October 25, 2024.
Available at: https://www.es.amnesty.org/en-que-estamos/paises/pais/show/tunez/.

109 **Freedom in the World 2023 Report.** Freedom House.
Available at: https://freedomhouse.org/country/tunisia/freedom-world/2023

110 **Swissinfo**. "The Arab Spring: the first smartphone revolution." 21 January 2020.
https://www.swissinfo.ch/spa/la-primavera-%C3%A1rabe-la-primera-revoluci%C3%B3n-smartphone/46193332.

111 **Ben Mhenni, Lina.** "Tunisia: 404 not found." Global Voices Advox. 24 September 2008.
Available at: https://advox.globalvoices.org/2008/09/24/tunisia-404-not-found

systematically intercepted using deep packet inspection (DPI) technologies[112] [113], which the Tunisian Government allegedly obtained from the US companies Blue Coat System and Netapp and the German company Utimaco, as later made public by human rights defenders[114]. On the other hand, Trovicor, a former subsidiary of Siemens AG and Nokia Siemens, based in Munich, reportedly provided the government with technologies enabling its use for voice and data interception and improved eavesdropping tools[115]. According to Privacy International, Sundby ETI A/S, a Danish company and a subsidiary of BAE Systems, reportedly sold mobile phone data interception technology capable of tracking[116] users' browsing habits and logging emails[117].

After the fall of the autocrat in 2011, the Tunisian Internet Agency (ATI), which promoted the development of the Internet in the country, was taken over by Moez Chakchouk, who dismantled the regime's digital surveillance apparatus and replaced it with a policy of openness and democratisation of access to the internet[118]. However, the dynamic of change did not last long. In 2013, the Agency for Telecommunications (ATT) was formed, which operates under the Ministry of Communications and Information Technologies and "provides technical support for judicial investigations into communication-related crimes"[119]. Internet activists such as Afef Abrougui warned at the time that the pretext of the fight against terrorism to control information on the Internet was enjoying a revival[120]. The return to the previous government's dynamics of surveillance and control would be reinforced in 2015, following a wave of attacks against tourists

112 See glossary.

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

114 **Goupy, Marie**. "La bienveillante neutralité des technologies d'espionnage des communications: le cas tunisien." *Cultures & conflits*, no. 93. 8 July 2014.
Available at: https://journals.openedition.org/conflits/18863

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

116 "Tracking" is a term that comes from "to track" and refers to the act of following, monitoring or recording the location, behaviour or activity of something or someone.

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

118 **El Dahshan, Mohamed**. "Hacking in Ben Ali's Basement'. Foreign Policy, 26 June 2013.
Available at: https://foreignpolicy.com/2013/06/26/hacking-in-ben-alis-basement/

119 Decree 2013-4506 adopted on 6 November 2013. Article 2.

120 **Abrougui, Afef**. "Tunisians cast a wary eye on new crime agency - Index on Censorship". Index on Censorship, 2 January 2014.
Available at: https://www.indexoncensorship.org/2014/01/tunisians-cast-a-wary-eye-on-att/.

"The lack of transparency in the public procurement of technology makes it impossible to know precisely which Ben Ali regime surveillance technologies are still being used by subsequent and current governments"

perpetrated by the self-styled Islamic State[121]. Shortly afterwards, the Counter-Terrorism Law 2015/26 was passed, harshly criticised by local and international human rights organisations, who considered that the new decree opened the door again to mass monitoring and surveillance[122]. A state of emergency was also declared that year and has remained in place for the last decade. The lack of transparency in the public procurement of technology makes it impossible to know precisely which Ben Ali regime surveillance technologies are still being used by subsequent and current governments[123].

2. CURBING FREEDOM OF EXPRESSION UNDER THE PRETEXT OF CYBERCRIME AND FAKE NEWS[124]

Since President Kaïs Saïed came to power in 2019, the siege against human rights defenders and voices opposing the government has intensified alarmingly. In 2020, Amnesty International published a report on the cases of 40 bloggers, administrators of popular Facebook pages and human rights defenders who were convicted on charges such as defamation, contempt of state institutions and "harming" others through social media. The NGO expressed concern about the growing tendency to compromise freedom of expression on social media using the regime's legal and punitive architecture[125]. This is the case of Tunisian blogger Emna Chargui, who posted a satirical text on Facebook about COVID-19 and confinement measures in the form of a verse from the Koran. In addition to

121 **BBC News**. "Tunisia attacks: Militants jailed over 2015 terror". 9 February 2019.
Available at: https://www.bbc.com/news/world-africa-47183027

122 **Human Rights Watch**. "Tunisia: Counterterror Law Endangers Rights". 31 July 2015.
Available at: https://www.hrw.org/news/2015/07/31/tunisia-counterterror-law-endangers-rights

123 **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".
Available at: https://ccprcentre.org/files/documents/INT_CCPR_ICS_TUN_30055_E.pdf

124 See glossary.

125 **Amnesty International.** *Tunisia: Criminal Prosecutions of Online Speech: Outdated and Flawed Laws Used to Restrict Speech in Tunisia.*
Available at: https://www.amnesty.org/en/documents/MDE30/3286/2020/en/

receiving death threats and threats of sexual violence (a frequently used attack against LGBTIQ+ people) from unidentified individuals, Chargui was sentenced to six months in prison for "offending religious feelings", while the threats she suffered have not been investigated[126].

This trend accelerated dramatically in 2021 when 60 human rights organisations denounced a wave of repression against Tunisian human rights defenders, which included the murder of two people and around 2,000 arrests in just 2 months, plus numerous cases of police harassment through social media, the sentencing to 6 months in prison of queer activist Rania Amdouni and the torture of young people in police stations[127]. President Saïed took advantage of the unrest in the streets, partly catalysed by the restrictive measures enacted during the COVID-19 pandemic, to freeze the activity of Parliament and dissolve the government, giving himself full constitutional powers because Tunisia was on the verge of "imminent danger"[128].

In 2022, a new Constitution was adopted that allowed suspending the right to privacy, enshrined in the 2014 Constitution, if the country was under a "state of emergency"[129]. This emergency was in force when the new text was adopted and extended by decree until December 2024[130]. Shortly afterwards, Decree Law No. 2022-54 of 13 September 2022 was passed, the so-called 'Cybercrime Law', which punishes the malicious dissemination of false information through digital networks. This law uses ambiguous terms, such as "fake news"[131], and gives authorities the power to shut down media outlets and civil society organisations in case of violation of its articles[132]. The law establishes provisions

126 **Amnesty International**. *Tunisia: Blogger Emna Chargui sentenced to six months in prison for social media post*. 9 November 2020.
Available at:
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.

127 **Nawaat**. *Avec le gouvernement Mechichi, l'Etat policier renaît de ses cendres*. 11 March 2021.
Available at:
https://nawaat.org/2021/03/11/avec-le-gouvernement-mechichi-letat-policier-renait-de-ses-cendres/

128 **France 24**. *Tunisia: President Kaïs Saïed suspends Parliament and dismisses Prime Minister Hichem Mechichi*. 25 July 2021.
Available at:
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

129 **Privacy International**. *State Surveillance in Tunisia*. 2019.
Available at: https://www.privacyinternational.org/state-privacy/1012/state-surveillance-tunisia

130 **Europa Press**. *Tunisia's president announces the extension of the long state of emergency for another year*. 21 January 2024.
Available at:
https://www.europapress.es/internacional/noticia-presidente-tunez-anuncia-ampliacion-otro-ano-mas-largo-estado-emergencia-20240131024235.html

131 See glossary.

132 **Amnesty International.** *La Tunisie doit abroger le décret relatif à la cybercriminalité*. 12 December 2022.
Available at: https://www.amnesty.org/es/documents/mde30/6290/2022/fr"

to allow authorities to "collect electronic evidence", collect personal data and intercept private communications based on vague criteria. Since then, more than 40 people have been arbitrarily detained for their advocacy or freedom of expression, the bulk of them for "conspiracy" under the Anti-Cybercrime Law. Most have been remanded in custody for months awaiting trial, in some cases for over a year[133].

"in the name of the fight against cybercrime is mainly targeted at young people, who in Tunisia have been the catalyst for significant mobilisations in the wake of the Arab Spring due to the lack of employment and prospects"

This repression in the name of the fight against cybercrime is mainly targeted at young people, who in Tunisia have been the catalyst for significant mobilisations in the wake of the Arab Spring due to the lack of employment and prospects. One of the best-known cases is that of student Ahmed Hamada, who ran a Facebook page where police abuses against the working-class neighbourhood of Hay Tadhamon in the capital were posted. Hamada was arrested in October 2022, and his computer and mobile phone were seized for data mining. He faces up to 12 years in prison for "using communication systems to spread fake news against state agents intentionally"[134].

133 **Human Rights Watch**. *Tunisie : Un décret sur la cybercriminalité utilisé contre les détracteurs des autorités.* 19 December 2023. Available at: https://www.hrw.org/fr/news/2023/12/19/tunisie-un-decret-sur-la-cybercriminalite-utilise-contre-les-detracteurs-des"

134 **The International Commission of Jurists - ICJ**. *Tunisia: Silencing Free Voices*. July 2023. Available at: https://www.icj.org/wp-content/uploads/2023/07/Tunisia-Silencing-Free-Voices-_compressed-1.pdf

3. INTERCEPTING COMMUNICATIONS AND HACKING DEVICES

In addition to the Cybercrime Law, the renewal of the state of emergency in 2023 granted the Tunisian Telecommunications Agency (ATT) access to electronic device contents without a warrant[135], giving it full powers to confiscate devices, extract data, and intercept communications.

In February 2024, 17 people from opposition parties, state officials and members of the "Citizens Against the Coup" initiative (which calls for an end to the state of emergency under the 2015 anti-terrorism law) were indicted on charges of conspiring to overthrow President Saïed. Some of the accused had their mobile phones and even storage cards confiscated, according to an investigation by the critical media outlet Inkyfada, which had access to the court file. During the interrogations, extracts from WhatsApp, Telegram, and even Signal[136], conversations they allegedly had with foreign diplomats were also used.

As in the rest of the region, one of the main targets of interception of communications in Tunisia is LGBTIQ+ people, where same-sex sexual practices are punishable by up to 3 years in prison[137]. The digitisation of relationships in the country has brought with it the criminalisation of so-called "digital immorality", which has materialised in the hyper-surveillance and exposure of data and intimate information of dozens of LGBTIQ+ people[138]. One of the growing trends in this regard is extracting information from devices, whether through non-consensual access, hacking, or threats. Human Rights Watch recounts the case of a male couple who were interrogated about their LGBTIQ+ activism by police officers, who demanded to see their conversations and Facebook pages. Despite their refusal, the officers confessed that they had already accessed this information through their landlord, who granted access to their Wi-Fi so they could

135 **Freedom House**. 2023. Available at: https://freedomhouse.org/country/tunisia/freedom-world/2023

136 **Issa, Ziadia**. "Enquête: "Complot contre la sûreté de l'État" : des dossiers vides pour éliminer l'opposition." inkyfada.com. 24 March 2023.
Available at: https://inkyfada.com/fr/2023/03/24/complot-surete-etat-dossiers-opposition-tunisie/.

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

138 **Human Rights Watch**. "Tunisie : Arrestations arbitraires d'activistes LGBTI et violences policières." 23 February 2021.
Available at:
https://www.hrw.org/fr/news/2021/02/23/tunisie-arrestations-arbitraires-dactivistes-lgbti-et-violences-policieres.

access their Wi-Fi and hack into their email accounts, phones, and laptops[139], collecting a large amount of private information.

In addition, LGBTIQ+ activism faces attacks by trolls or electronic armies[140], organised on social media, which denigrate and incite violence against them. In 2021, a group of human rights defenders who flew the rainbow flag at a demonstration in the Tunisian capital were subjected to online harassment, in some cases by Facebook pages associated with police unions. This is the case of lesbian artist Rania Amdouni, of whom hundreds of photographs were circulated with death threats and whose address and phone number were leaked by trolls[141] [142]. In some cases, these people even flee the country because of the insecurity they feel (sexile).

4. BILLION-DOLLAR WESTERN INVESTMENT IN BORDER SURVEILLANCE

Much of the more sophisticated technology used by the government is channelled into surveillance of the Tunisian coast and the border with Libya to monitor not only migration to Europe but also the presence of violent Islamist groups, especially after the 2015 attacks. From 2016 to 2018, the government built a 200-kilometre wall along its border with Libya, equipped with high-resolution and long-range systems and thermal and motion-detection cameras linked to a surveillance centre. The project was funded by Germany[143] and the United States[144], and implemented by URS, a subsidiary of the multinational engineering company AECOMS (both are American companies) [145] [146].

---

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

140 See glossary.

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

142 See glossary.

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

144 **Kapitalis**, Webmaster. "Des Américains installent la surveillance électronique au sud de la Tunisie," 14 August 2016. Available at: https://kapitalis.com/tunisie/2016/08/14/des-americains-installent-la-surveillance-electronique-au-sud-de-la-tunisie.

145 Ibid.

146 **Webdo**. *Le système de surveillance électronique à la frontière tunisienne-libyenne, installé en 2018.* Available at: https://www.webdo.tn/fr/actualite/national/systeme-de-surveillance-electronique-a-frontiere-tuniso-libyenne-installe-2018/158669

"The restrictions on freedom of movement for people migrating from Tunisia have worsened in recent years, accompanied by racist campaigns of harassment and defamation on social media"

Recently, the government has acquired a sophisticated digital recognition and biometric identification system provided by the French giant Idemia[147]. The justification for implementing these systems is to reinforce technical and operational capacities in border security and the pursuit of "terrorist" groups. The restrictions on freedom of movement for people migrating from Tunisia have worsened in recent years, accompanied by racist campaigns of harassment and defamation on social media, fuelled by President Saïed himself[148]. There have also been reports of violence, including sexual violence against migrants, as recently published by The Guardian[149]. Since 2013, the Tunisian Ministry of Interior has imposed movement restrictions on nearly 30,000 people via border control measures. Said borders are not publicly accessible and completely lack judicial oversight, as Amnesty International denounced in a report published in 2018[150].

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

148 **Amnesty International**. "The racist rhetoric of the President of Tunisia incites a wave of violence against Black Africans." Published March 14th, 2023.
Available at:
https://www.amnesty.org/en/latest/news/2023/03/tunisia-presidents-racist-speech-incites-a-wave-of-violence-against-black-africans/

149 **The Guardian**, "The brutal truth behind Italy's migrant reduction: beatings and rape by EU-funded forces in Tunisia," 19 September 2024.
Available at:
https://www.theguardian.com/global-development/2024/sep/19/italy-migrant-reduction-investigation-rape-killing-tunisia-eu-money-keir-starmer-security-forces-smugglers

150 **Amnesty International**, "Tunisia: Arbitrary and abusive travel restrictions violate human rights," 24 October 2018.
Available at:
https://www.amnesty.org/es/latest/press-release/2018/10/tunisia-arbitrary-and-abusive-travel-restrictions-breach-human-rights/

IV

EGYPT: THE STATE AS MALICIOUS HACKER AND ONLINE HARASSER

When the Arab Spring hit Cairo's Tahrir Square in 2011, the Mubarak Government expanded the technology available to intercept phone calls and tighten the siege against human rights defenders fighting against the regime. In 2016, a Privacy International report revealed the existence of a secret unit, the Technical Research Department (TRD), attributed to the Egyptian General Intelligence Service, which reportedly purchased surveillance technology from Finland's Nokia Siemens Network[151]. After the military coup by the president of the Supreme Council of the Armed Forces, Abdul Fatah al-Sisi, against the then-elected President Mohamed Morsi in 2013, not only did the situation worsen in terms of freedom of expression and political rights, but internet freedom and users' rights were severely restricted, as the Freedom on the Net report 2023 points out[152]. Criminal sanctions, harassment and surveillance have contributed to making journalism critical of the government impossible, fuelling censorship and self-censorship.

Egyptian security agencies have acquired sophisticated technology for spying, monitoring and intercepting communications from Western companies, a strategy they have implemented thoroughly while developing a surveillance industry[153]. Massive censorship of websites, estimated at more than 600 sites blocked since 2017, and the persecution and harassment of journalists, human rights defenders and LGBTIQ+ people have turned the North African country into a prolific client and a veritable laboratory for Western companies' mass surveillance and online monitoring technologies.

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

152 **Freedom House.** "Freedom on the Net 2023, Country: Egypt."
Available at: https://freedomhouse.org/country/egypt/freedom-net/2023.

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

1. CREDENTIAL THEFT AND FRAUDULENT ACCESS TO HUMAN RIGHTS NGOS EMAIL ACCOUNTS

In Egypt, the Al Sisi Government is highly active in the digital harassment of civil society if one looks at the number of reports and complaints from human rights defenders that have been made public in recent years. This is not limited to the classic interception of communications via messaging or phone apps but uses all available means. In 2017, a phishing campaign[154] called "Nile Phish" was uncovered against at least seven human rights NGOs and human rights defenders, lawyers and journalists in the country[155]. According to an investigation by the Citizen Lab organisation, this hacking technique resulted in dozens of Gmail and Dropbox[156]. accounts being hacked. In this case, victims were infected via a fake email from the organisation Nadeem Center for Rehabilitation of Victims of Violence (since shut down by the Egyptian authorities) and invited to open a link for more information on a supposed conference. The attack was orchestrated using a free, open-source platform called GoPhish, which allows for creating realistic simulations of trusted users.

"the Al Sisi Government is highly active in the digital harassment of civil society"

In March 2019, Amnesty International research uncovered another wave of digital attacks that "likely originated from government-backed agencies"[157] and involved multiple attempts to gain access to the email accounts of several Egyptian human rights defenders, media and staff of Egyptian organisations. This new campaign came amid what the NGO said was an "unprecedented crackdown that has turned Egypt into an 'open-air' prison for critics"[158]. In this case, the attackers did not use traditional phishing methods[159] to steal

154 See glossary.

155 **Withaker, Bryan.** "How the Middle East Became an Electronic Battleground." Hackernoon. 19 June 2017. Available at: https://hackernoon.com/how-the-middle-east-became-an-electronic-battleground-dac5b5435eb.

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

157 **Amnesty International.** "Phishing attacks using third-party applications against Egyptian civil society organizations". 6 March 2019. Available at: https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

158 Ibid.

159 See glossary.

credentials. They used a stealthier and more efficient way to access victims' inboxes: a technique known as OAuth Phishing[160], which tricks users into granting permissions to malicious applications that can access their account data and perform actions on their behalf. The attackers tricked victims into granting them full email access via mobile apps hosted on Google's and Android's official Play Store[161].

According to a report published months later by Check Point Research, the intelligence platform of Israeli company CheckPoint Software Technologies, the attack affected 33 journalists, politicians, lawyers and human rights defenders, whose emails, contacts and locations were intercepted and recorded[162]. CheckPoint did not find a direct and irrefutable link to Egyptian intelligence services, although the platform considered that given "the targets, the clear intent and purpose of the applications, the structure and data downloaded, as well as a server registered with the Ministry of Information Technology and an encrypted location corresponding to the headquarters of Egypt's main spy agency, it is almost certain that this was a government-driven action"[163].

"The attackers tricked victims into granting them full email access via mobile apps hosted on Google's and Android's official Play Store"

160 See glossary.

161 **Checkpoint Research.** "The eye on the Nile." 2019. Available at: https://research.checkpoint.com/2019/the-eye-on-the-nile/.

162 **Checkpoint Research.** "The eye on the Nile." 2019. Available at: https://research.checkpoint.com/2019/the-eye-on-the-nile/.

163 Ibid

2. ESPIONAGE AND DATA MINING WITH ISRAELI TECHNOLOGY AND CAPITAL

Between May and September 2023, former Egyptian parliamentarian Ahmed Eltantawy was the target of several attempts to infect his mobile phone with the spyware[164] Cytrox's Predator after announcing his intention to run in the 2024 presidential elections[165]. This software allows real-time monitoring[166]. of infected devices, regardless of their location. Cytrox is part of the Intellexa Consortium, a group of spywares[167] and related services companies known for competing with NSO Group and selling technology to countries where NSO no longer sells its products after scandals related to its impact on human rights violations[168]. In March 2024, the US Treasury Department sanctioned Cytrox, the Intellexa Consortium and its CEO Tal Dilian, a former member of the Israeli army's technology development units for 25 years, for selling espionage and mass surveillance tools to authoritarian regimes and "for their role in the development and distribution of spyware[169] used against US citizens, including members of the government, journalists and advisors"[170].

Eltantawy's mobile connection was persistently attacked via network injection[171]. When he visited certain websites that did not use HTTPS, a device installed at the border of Vodafone Egypt's network automatically redirected him to a malicious website to infect his phone with spyware while receiving links via SMS and WhatsApp to make it easier for him to fall into the trap. The former MP, who suspected that he might be the victim of an attempted infection, contacted the Citizen Lab platform[172] In the statement confirming Eltantawy's

164 See glossary.

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

166 **Sekoia.io.** "Predator spyware." Available at: https://www.sekoia.io/en/glossary/predator-spyware/.

167 See glossary.

168 **Red en Defensa de los Derechos Digitales.** "US sanctions CEO of spyware maker Intellexa for human rights violations."
Available at:
https://r3d.mx/2024/03/20/estados-unidos-sanciona-al-ceo-de-intellexa-empresa-creadora-de-spyware-por-violaciones-a-derechos-humanos/.

169 See glossary.

170 **US Department of Treasury.** "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium". 05 March 2024. Available at: https://home.treasury.gov/news/press-releases/jy2155.

171 See glossary.

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

suspicions, Citizen Lab claimed that "given that Egypt is a known customer of Cytrox's Predator spyware, and that the spyware was delivered via network injection[173] from a device physically located inside Egypt, we attribute the network injection attack to the Egyptian Government with high probability"[174]. During the same period, security forces arrested several of his campaign volunteers[175].

3. CANADIAN TECHNOLOGY FOR CENSORING CRITICAL WEBSITES

Large-scale website censorship, in addition to a regional trend, is a prominent dynamic in the Egyptian context. Since 2017, more than 600 websites and domains have been inaccessible from within the country. This phenomenon was denounced in 2020 by Egyptian, regional and international organisations such as the Cairo Institute for Human Rights Studies (CIHRS) or the Electronic Frontier Foundation (EFF), which pointed out that this dynamic constitutes a violation of the right to access information and freedom of expression[176]. The websites belong to critical media and political platforms that denounce human rights violations, such as the social journalism media Al-Manassa, which has suffered persecution and blocking since shortly after its

"Large-scale website censorship, in addition to a regional trend, is a prominent dynamic in the Egyptian context. Since 2017, more than 600 websites and domains have been inaccessible from within the country."

173 See glossary.

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

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

176 **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 November 2021.
https://ifex.org/human-rights-organizations-call-on-egypts-government-to-end-internet-censorship-and-website-blocking/

creation in 2016[177]. Egyptian authorities have even blocked alternative domains that the site used to continue operating. In June 2020, security forces raided the offices of Al-Manassa[178]. and arrested its editor-in-chief, Nora Younis, who was detained for three days on charges of operating an unlicensed site and committing cybercrimes before being released on bail. Younis became the first Egyptian journalist to face charges under the cybercrimes law, despite Al-Manassa having applied for a license and paid the corresponding fees in 2018[179] [180] [181].

The restriction of access to certain content and the closure of websites was carried out by invoking the Media and Press Regulation Law and the Cybercrime Law passed in 2018, which expands powers for online surveillance, website blocking, interception of communications and internet monitoring[182]. Article 7 of the Cybercrime Law gives the investigating authority the power to shut down a website whenever it considers that the content constitutes a crime or a threat to national security or the economy.

Al-Manassa enlisted the digital forensics services of Swedish digital rights, data protection and internet security NGO Qurium[183], whose research revealed that Egyptian internet providers use deep packet inspection (DPI)[184] to restrict access to certain content and websites. According to US tech digital media outlet The Verge, deep packet inspection is one of the most invasive technologies a country can use on its internet network. "This

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

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

179 **CPJ Middle East.** "Al-Manassa Editor Nora Younis on Censorship in Egypt." Committee to Protect Journalists. October 26th, 2020.
Available at: https://cpj.org/2020/10/al-manassa-editor-nora-younis-on-censorship-in-egypt/

180 **MPC Journal.** "Egypt Arrests Another Independent Media Journalist." Middle East Politics and Culture Journal. June 25th, 2020.
Available at: https://mpc-journal.org/egypt-arrests-another-independent-media-journalist/

181 **The Street Journal.** "Egypt: Al-Manassa Editor Nora Younis on Censorship in Egypt." The Street Journal. June 25th, 2020.
Available at: https://thestreetjournal.org/egypt-al-manassa-editor-nora-younis-on-censorship-in-egypt/

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

183 **Qurium.** "How Operators Use Sandvine to Block Independent Media in Egypt." Qurium Media Foundation. September 7th, 2020.
Available at: https://www.qurium.org/press-releases/how-operators-use-sandvine-to-block-independent-media-in-egypt/

184 See glossary.

technique, employed by authoritarian regimes from Russia to Bahrain, allows governments to examine the content of web traffic as it moves across the network, enabling them to censor websites in real-time and conduct detailed surveillance of civil society's online activities. It also requires sophisticated equipment, which a Western company usually provides"[185], says the online media.

In this case, the company was Sandvine[186], a Canadian company that, from 2017 until August 2024, was owned by the investment group Francisco Partners, also a shareholder of NSO Group until 2019. In February 2024, it became public that the US Treasury Department had listed Sandvine for the involvement of its DPI technology[187] in online censorship and spying on human rights defenders in Egypt[188]. Following the scandal, Francisco Partners decided to dispose of Sandvine, which is currently for sale for $450 million[189].

4. HARASSMENT CAMPAIGNS AND DIGITAL AMBUSHES AGAINST HUMAN RIGHTS DEFENDERS[190]

Another common surveillance mechanism used against human rights defenders is social media harassment, often fuelled by bots. This siege tends to intensify at times when the media spotlight is focused on Egypt, and the regime cannot afford to let the situation of suffocating authoritarianism spread beyond its borders.

In December 2020, a vilifying hashtag against the director of the Egyptian Initiative for Personal Rights (EIPR), Hossam Bahgat, went viral in the country, filling the X network (formerly Twitter) with homophobic and dehumanising content. The attack, followed by

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

186 **Lyons, Jessica.** "Sandvine Put on America's Export No-Fly List after Egypt Used Network Tech for Spying." *The Register.* 27 February 2024. Available at: https://www.theregister.com/2024/02/27/

187 See glossary.

188 **United States Department of State.** "The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses." 28 February 2024.
Available at:
https://www.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-ab

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

190 See glossary.

hundreds of trolls[191] and bots, some of them pro-government[192], was part of a broader offensive against the staff of this Egyptian human rights organisation. Three of the NGO's staff were arrested in the same period, following a visit by 13 diplomats to the organisation's headquarters, and released two days later[193].

"a vilifying hashtag against the director of the Egyptian Initiative for Personal Rights (EIPR), Hossam Bahgat, went viral in the country, filling the X network (formerly Twitter) with homophobic and dehumanising content. The attack, followed by hundreds of trolls and bots, some of them pro-government"

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

This was not the only method of harassment against Bahgat. In January 2019, after he made a critical tweet, hundreds of fake accounts started following his account on X every minute for a few days. Far from being innocuous, that attack technique usually leads to account closure or suspension because it is associated with bot behaviour.

In the weeks leading up to the COP27 climate summit in 2022, more than 150 people were arrested and investigated by the Egyptian State Security High Prosecutor's Office for using social media to call for protests at the summit[194]. It was also published that the COP27 mobile app, developed by the Egyptian Ministry of Communications and Information Technology, allowed authorities to listen to conversations, access private emails, and track messages, including encrypted ones[195]. The app was labelled a "cyber weapon", although it could not be proven that such surveillance was happening.

191 See glossary.

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

193 **FrontLine Defenders.** Crackdown on Egyptian initiative for personal rights staff.
Available at: https://www.frontlinedefenders.org/en/case/crackdown-egyptian-initiative-personal-rights-staff

194 **Coogle, Adam.** "Egypt: Arrests, Curbs on Protests as COP27 Nears". Human Rights Watch. 6 November 2022.
Available at: https://www.hrw.org/news/2022/11/06/egypt-arrests-curbs-protests-cop27-nears

195 **Scott, Mark, and Vincent Manancourt.** "Egypt's COP27 Summit App Is a Cyber Weapon, Experts Warn". POLITICO. 9 November 2022.
Available at: https://www.politico.eu/article/cop-27-climate-change-app-cybersecurity-weapon-risks

As elsewhere in the region, but particularly violently in Egypt, LGBTIQ+ people continue to be a prime target for online harassment and repression. From the end of 2013 to 2017, the annual average number of arrests was 66, while in 2019, there were 92 arrests of people suspected of homosexual practices[196]. The use of dating apps such as Grindr, Hornet and Growler, common among LGBTIQ+ people, has become a source of risk, combined with the extreme level of online and offline surveillance. This is the case of a gay man who was detained in 2018 for 11 days after being set up in a trap where a police officer contacted him, making him believe he had a romantic interest, then stopped him at a checkpoint and forced him to show the contents of his mobile phone[197]. Additionally, following the passage 2018 of the Cybercrime Act, cases against LGBTIQ+ persons are judged not only as morally wrong but also as a cybercrime offence, allowing authorities to impose harsher sentences and stricter penalties[198].

196 **Afsaneh Rigot.** "Egypt Has a New Tool for Persecuting LGBTQ People," *Slate*. 30 Dec. 2020. Available at: https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html.

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

198 **Afsaneh Right.** Egypt has a new tool for persecuting LGBTQ people. 30 December 2020. Available at: https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html.

V

LEBANON: CYBER-ESPIONAGE, CENSORSHIP AND DIGITAL VIOLENCE

The 2011 Arab Spring in Lebanon sowed the seeds of outrage that germinated into massive popular uprisings in subsequent years. The popular mobilisations of 2011 demanded an end to the confessional and sectarian system in the country but only lasted for three months[199]. Despite this, the indignation remained latent, and new campaigns gradually emerged, such as those in 2013 (#NoToExtension) and 2015 ("YouStink"). It was in this framework that the slogan "All Means All" began to be used, which would give visibility and meaning to the 2019 protests against the government and the banking system, with the active participation of migrant and domestic workers[200], many of whom work in the country in a regime of semi-slavery[201]. This process represented the emergence of a new generation of human rights defenders who skilfully combined new digital technologies to organise social mobilisation.

In response to this popular surge, the government reinforced mass surveillance systems. In 2018, a sophisticated cyber-espionage infrastructure known as Dark Caracal, linked to the Lebanese General Directorate of General Security (GDGS), came to light. Since 2012, it has launched multiple mass surveillance campaigns using advanced technologies from Western companies[202]. The civil and digital rights of the Lebanese population are also under threat due to a restrictive and weak regulatory framework in protecting the right to privacy. On the other hand, because of the vulnerability of the country's digital infrastructure, as demonstrated during the cyber-attack against the passenger registration platform (MOPHPASS) created by the Ministry of Health to manage COVID-19[203]. More recently, the massive attack against Hezbollah militants' pagers and walkie-talkies has also demonstrated Israel's technological capacity to attack Lebanese territory[204].

---

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

200 **France 24.** Foreign domestic workers in Lebanon protest abuses. France 24. 5 May 2019.
Available at: https://www.france24.com/en/20190505-foreign-domestic-workers-lebanon-protest-abuses

201 **Kvinna till Kvinna**. *Abolishing modern slavery in Lebanon.* Kvinna till Kvinna. 27 March 2023.
Available at: https://kvinnatillkvinna.org/2023/03/27/abolishing-modern-slavery-in-lebanon/

202 **The Hacker News.** *Researchers Uncover Government-Sponsored Mobile Hacking Group Operating Since 2012*. 19 Jan. 2018.
Available at: https://thehackernews.com/2018/01/dark-caracal-android-malware.html.

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

204 **ElDiario.es.** Israel planted explosives in thousands of beepers imported by Hezbollah and accelerated the attack for fear of being discovered. 18 September 2024.
Available at:
https://www.eldiarioar.com/mundo/israel-coloco-explosivos-miles-buscas-importados-hizbula-acelero-ataque-temor-descubierto_1_11663562.html

1. MASSIVE CYBER ESPIONAGE ON THE POPULATION

In the last 20 years, internet usage in Lebanese society has increased from 9% to 90%[205]. By the end of 2021, around 4.2 million Lebanese, approximately 76% of the total population, were mobile phone subscribers[206]. In this context, Lebanon's leading intelligence agencies, such as the GDGS, the Ministry of Interior's Internal Security Forces (ISF), and the Ministry of Defence's Directorate of Military Intelligence (MID), each have their surveillance systems, especially technologies for intercepting communications[207]. The MID also has systems for monitoring and extracting data from social networks. In addition, the UK supports the MID under the 'Prevent' strategy to counter violent extremism[208].

Interception of telecommunications is a common practice of Lebanese intelligence agencies. In theory, Law 140/1999 on Interception of Communications states that personal communications (telephone, fax, emails) are protected under the law and can only be intercepted in cases of extreme urgency and under judicial or administrative order[209]. However, in practice, these judicial guarantees do not occur. According to Privacy International, there is no guarantee that state intelligence services carry out mass interception of communications without any legal oversight[210]. Since the assassination of Prime Minister Rafiq Hariri in 2005, the ISF has, on several occasions and under the authorisation of the Lebanese Council of Ministers, been given unlimited access to telecommunications data of Lebanese society[211].

In parallel, Lebanese intelligence services have been acquiring technologies and services from Western companies for mass surveillance of civil society since the Arab Spring. In 2015, for $1.4 million, the MID acquired the mass surveillance software 'Remote Control System' from the Italian company Hacking Team, which allowed it to record audio, take

205 **DataReportal.** (2024). *Digital 2024: Lebanon.* DataReportal.
Available at: https://datareportal.com/reports/digital-2024-lebanon

206 **CEIC Data.** *Lebanon number of mobile subscribers.*
Available at: https://www.ceicdata.com/en/indicator/lebanon/number-of-subscriber-mobile

207 Digital analyst, interview by research team, 9 September 2024.

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

209 **Privacy international.** State of privacy Lebanon. 27 January 2019.
Available at: https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

210 Ibid.

211 Ibid.

screenshots of mobile phones, and monitor the GPS location of mobile phones[212]. Similarly, the University of Toronto's research centre, Citizen Lab, reported using spyware[213] FinFisher from the British company Gamma Group to infect computers and obtain the information they contain. According to the centre, the ISF and GDGS intelligence agencies used this technology in 20155[214].

"poor media literacy in Lebanon exposes civil society to phishing and spyware on their mobile devices and computers."

However, the Dark Caracal infrastructure was the most extensive system used for mass surveillance in Lebanon. In 2018, the organisation's Lockout and Electronic Frontier Foundation (EFF) published the report "Dark Caracal - Cyber-espionage on a Global Scale," describing a massive cyber-espionage system with Advanced Persistent Threat (APT) capabilities[215] managed from a GDGS building in Beirut since 2012[216]. Specifically, Dark Caracal launched regular 'surveillance campaigns' combining traditional hacking systems with advanced mass surveillance systems such as the so-called Pallas or FinFisher's[217] spyware, capable of extracting information from SMS, messaging apps, screenshots, audio recordings, Wi-Fi hotspot locations and SSIDs[218]. According to EFF and Lockout, this system obtained hundreds of gigabytes of information from financial institutions, corporations, security and defence contractors, military, educational institutions, journalists, lawyers and human rights defenders in more than 21 countries[219]. In this regard, Ralph Baydoun, a Lebanese digital analyst, adds that poor media literacy in Lebanon exposes civil society to phishing[220] and spyware[221] on their mobile devices and computers[222].

212 **Ambri, Anas and Andrea Glioti.** "Spyware Brokers and Lebanon's Surveillance State" *The New Arab*. 21 November 2023.
Available at: https://www.newarab.com/investigations/spyware-brokers-and-lebanons-surveillance-state

213 See glossary.

214 **Bill Marczak et al.** "Mapping FinFisher's Continuing Proliferation" *The Citizen Lab*. 15 October 2015.
Available at: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

215 See glossary.

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

217 See glossary.

218 The acronym SSID stands for Service Set Identifier. It is the name of a Wi-Fi network so that it can be found and identified among other networks and connections.

219 Ibid.

220 See glossary.

221 See glossary.

222 Ralph Baydoun, personal interview conducted by the research team, 6 September 2024.

However, despite these advanced espionage systems, the country's cyber security architecture is fragile. Government websites and critical infrastructure are systematically hacked in Lebanon. Recent examples include the hacking of Beirut International Airport's information boards[223], or the websites of the Ministry of Social Affairs and the Lebanese Parliament by a group of hackers allegedly hired by Israeli actors[224]. According to Lebanese investigative journalist Imad Bazzi, this situation highlights the country's cybersecurity chaos. It also indicates the lack of sophisticated capabilities for comprehensive government population monitoring[225].

On the other hand, other national and international non-state actors are at play in the dynamics of mass surveillance targeting Lebanese society. The case of the[226] malware known as Flame, coming from Iran, to hack mobile phones and computers in 2012; or the use of the Zoopark malware, between 2015 and 2018, with the capacity to obtain data from SMS messages, internet browsing, GPS location, passwords, stand out among others. However, the most significant security breach in the country has been Israel's recent massive attack on Hezbollah militants through the explosion of their devices, pagers and walkie-talkies. The attack left 32 dead, including a child, and thousands injured across the country[227].

2. CONTROLLING DIGITAL FREEDOM OF EXPRESSION

Since the 2019 protests, the emergence of alternative media has been growing. Numerous female bloggers and independent digital media have created forms of communication that are closer to society. One of the key examples was the live broadcast, with stories and testimonies from the streets, during the explosion in the port of Beirut on 4 August 2020. New bloggers and independent media use social networks and blogs to disseminate their material. To silence these dissenting voices, the government monitors content in digital spaces.

---

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

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

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

226 See glossary.

227 **Matt Murphy and Joe Tidy.** "What We Know About the Hezbollah Device Explosions," BBC News. 20 September 2024. Available at: https://www.bbc.com/news/articles/cz04m913m49o.

Since 2006, the Cybercrime and Intellectual Property Rights Office, attached to the ISF's Special Criminal Investigations Department, has been prosecuting crimes involving information technologies. This office has been denounced for its censorship practices and abuses of freedom of expression, as well as press freedom for journalists, bloggers, and other public figures in the country[228]. Surveillance and persecution of journalists and bloggers are carried out through the defamation articles of the Penal Code (art.582-582, 383, 386) and the Law on Publications (art. 20-21). According to official data, the Cybercrime Bureau investigated between January 2019 and March 2024, 1,684 defamation cases[229].

In Lebanon, arrests, interrogations and intimidation of human rights defenders and journalists are common practice[230]. According to the Samir Kassir Foundation, more than 800 abuses against journalists have been recorded since 2018, including interrogations, coercion, harassment by telephone and physical violence by State Security Forces[231]. One relevant case was that of the journalist Jean Kassir of the digital media Megaphone in 2013, who was arrested and interrogated by the ISF under a defamation lawsuit for his criticism of political leaders in the case of the explosion in the port of Beirut[232]. In the same year, Lara Bitar of the online media the Office of Cybercrime summoned the Public Source for publishing an article on toxic waste in Lebanon[233]. Other sources report coercive practices such as threats to send malware[234] to monitor the activity of human rights defenders on social media[235]. Access Now also reports cases of coercion to force human rights defenders to cease their online activities by signing a pledge[236].

---

228 **Arabic Network for Human Rights Information et al.** *"Lebanese Bloggers Facing Threats."* 28 March 2014. Available at: https://ifex.org/lebanese-bloggers-facing-threats

229 **Amnesty International.** "*Lebanon: End Use of Defamation Laws to Target Journalists and Critics."* 33 May 2024. Available at: https://www.amnesty.org/en/latest/news/2024/05/lebanon-end-use-of-defamation-laws-to-target-journalists-and-critics/

230 **Melki, Jad, et al.** *"Mapping Digital Media: Lebanon."* Open Society Foundations, March 15, 2012. Available at: https://www.opensocietyfoundations.org/publications/mapping-digital-media-global-findings

231 **Ayyad, Safaa.** *"Lebanon: Summoning Journalists in Beirut and Silencing Voices in Mount Lebanon."* SMEX. 5 April 2023. Available at: https://smex.org/lebanon-summoning-journalists-in-beirut-and-silencing-voices-in-mount-lebanon/

232 **Christou, William.** *"Charges Dropped Against Lebanese Media Outlet Megaphone."* The New Arab. 4 April 2023. Available at: https://english.alaraby.co.uk/news/charges-dropped-against-lebanese-media-outlet-megaphone

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

234See glossary.

235 **Habib Battah.** "Who's Got Your Data?" *Beirut Report*. September 2024. Available at: https://beirutreport.com/whos-got-your-data-2/

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

In this vein, Imad Bazzi notes that the common practice is not the exhaustive monitoring of social media to identify "inappropriate" content. Instead, it is a process where elites who feel "annoyed" by a person's political activism contact a political party to activate a legal prosecution through the state prosecutor's office or trigger the mechanisms of the Cybercrime Office[237]. In most cases, these campaigns are not made public and human rights defenders simply disappear from the public arena and/or self-censor themselves[238].

The Cybercrime Office has extensive resources and technologies to monitor social networks and mobile hacking techniques. In this regard, in 2015, a proposed contract between the Office and the company Hacking Team was identified, where it is suspected that it was used to cyberspy on 50 people for 450,000 dollars[239]. In 2013, the Citizen Lab Centre reported the presence of PacketShaper technology from Blue Coat to monitor users' interactions with social networks, messaging and online communications[240]. Based on this monitoring of the digital space, the government blocks websites, blogs, and applications. In 2015, SMEX identified the closure of 45 websites linked to Israel, gambling, pornography, prostitution, but also LGBTIQ+ groups[241]. In 2018, the Ministry of Telecommunications blocked the website creation platform Wix[242] and, in 2020, the blogging website "Blogger" (*.blogspot.com). Similarly, in 2019, the dating application Grindr was also blocked without any information or justification from the Ministry of Telecommunications[243]. Instead of improving, the situation points to a toughening of penalties. The new proposed Media Law includes sentences of up to three years for defaming religions recognised in the country[244]. In response, Amnesty International

237 Imad Bazzi, personal interview conducted by the research team, 4 September 2024.

238 Ibid.

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

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

241 **SMEX.** "Mapping Blocked Websites in Lebanon 2015". 26 March 2015.
Available at: https://smex.org/mapping-blocked-websites-in-lebanon-2015/

242 **Mariam S.,** "Help Us to Map Blocked Websites in 2019". *SMEX.* 22 January 2019.
Available at: https://smex.org/help-us-to-map-blocked-websites-in-2019/

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

244 **Coalition to Defend Freedom of Expression.** "Proposed Media Law Poses Grave Threat to Freedom of Expression" *Legal Agenda.* 28 November 2023.
Available at:
https://english.legal-agenda.com/proposed-media-law-poses-grave-threat-to-freedom-of-expression/

launched a campaign in 2023 to reform Lebanon's defamation laws under the hashtag #MyOpinionIsNotaCrime[245].

3. FROM SOCIAL MEDIA SURVEILLANCE TO DIGITAL VIOLENCE

Police surveillance against queer people has intensified since 2019. This persecution combines mass digital surveillance with the identification of LGBTIQ+ people on public roads in the country's main cities. Article 542 of the Lebanese Penal Code criminalises same-sex relationships[246]. This criminalisation results in online surveillance and harassment of LGBTIQ+ people. The British organisation Article 19 claims that ISFs use the dating apps Grindr, Hornet, PlanetRomeo and Growl to collect evidence of homosexual behaviour to arrest and report these people[247]. In addition to this online harassment, LGBTIQ+ people are identified on public streets to confiscate and examine their mobile phones to find images and information in the library of photos or WhatsApp chats by the police to be used later in prosecutions[248].

The practice of seizing mobile phones, computers and other means of communication also occurs in Syrian refugee camps, accentuating the social isolation of these communities[249]. This practice by the State Security Forces has increased since the 2019 demonstrations. SMEX points out that there is no clear legal framework in this regard[250].

Criminalisation and physical harassment of LGBTIQ+ groups or refugees is justified through disinformation campaigns and online harassment. For example, since mid-2024, there has been an increase in hate speech on social media and mainstream media against Syrian refugees from the Lebanese Government, political leaders, religious leaders, and

245 **Amnesty International.** *"Campaign to Decriminalize Defamation and Insult in Lebanese Laws"*. 8 August 2023. Available at: https://www.amnesty.org/en/latest/campaigns/2023/08/campaign-to-decriminalize-defamation-and-insult-in-lebanese-laws/.

246 **Human Rights Watch.** "Lebanon: Same-Sex Relations Not Illegal". 19 July 2018. Available at: https://www.hrw.org/news/2018/07/19/lebanon-same-sex-relations-not-illegal

247 Arrest and Abuse of LGBTQ+ App Users in Lebanon: A Digital Rights Crisis. 2018. Available at: https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf

248 **Article 19.** Digital Crime Scenes: How Counterterrorism Laws Undermine Free Expression. March 2022. Available at: https://www.article19.org/wp-content/uploads/2022/03/Digital-Crime-Scenes-Report-3.pdf

249 **ACHR.** "Lebanon: Censorship and Violations of Free Speech". Arab Center for Human Rights. 13 January 2023. Available at: https://www.achrights.org/en/2023/01/13/12910/

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

“the country’s political elites have electronic armies of thousands of bots to develop massive disinformation campaigns and online harassment to attack the reputation of a group and/or person.”

even groups aligned with Hezbollah[251]. The digital analyst Ralph Baydoun details that the country’s political elites have electronic armies[252] of thousands of bots to develop massive disinformation campaigns and online harassment to attack the reputation of a group and/or person[253].

Reputational attacks on social networks are transferred to physical spaces, including aggressions and murders. One of the most paradigmatic cases related to reporting government corruption cases in 2019 had severe implications for the journalist’s physical and psychological integrity (as well as that of her family members)[254]. There were campaigns of digital violence and lawfare, hate speech and doxing[255]. The case also resulted in a one-year prison sentence for this woman defender on a defamation charge after she publicly denounced violence against human rights defenders by members of the Christian Free Patriotic Movement party. are particularly affected by digital violence. According to SMEX, between 2020 and 2023, 80% of the targets of digital violence in Lebanon were[256].

251 **Salhani, Justin.** “Targeted: How Misinformation Puts Lebanon’s Syrian Refugees in Danger” *The Tahrir Institute for Middle East Policy* (TIMEP). 28 August 2024. Available at: https://timep.org/2024/08/28/targeted-how-misinformation-puts-lebanons-syrian-refugees-in-danger/

252 See glossary.

253 Ralph Baydoun, personal interview conducted by the research team, 6 September 2024.

254 For reasons of security for the defender, the name and case references are omitted.

255 See glossary.

256 **Ayyad, Safaa.** “80% of Women in Lebanon Face Digital Violence” SMEX. 4 March 2024. Available at: https://smex.org/80-of-women-in-lebanon-face-digital-violence/

VI

THE SYRIAN WAR EXACERBATES MASS SURVEILLANCE

Cyberspace in Syria is heavily regulated and controlled by the government through various ministries and entities, most intensely since the events that occurred during the Arab Spring. The Syrian Government's security apparatus is composed of Syrian military intelligence, in which different units collaborate to exercise control and cyber surveillance over the population. Unit 225 is responsible for monitoring internal communications[257]. This unit has, among others, the ability to block specific numbers, terminate calls, and disable SMS services[258]. There is also Unit 211[259], known as the "technical" or "IT" branch, which focuses on regulating website access, managing wireless communications and providing technical support to Unit 225. Finally, Unit 237[260] specialises in monitoring and recording wireless calls.

"Cyberspace in Syria is heavily regulated and controlled by the government through various ministries and entities, most intensely since the events that occurred during the Arab Spring."

When widespread protests began in the Maghreb and Mashreq region, especially in Egypt and Tunisia, Syrian President Assad inferred that the protests had succeeded in toppling their leaders because the governments failed to suppress the demonstrations early enough. Assad's Government was already known before the war for censoring internet content in the country[261]. As soon as the protests began, Syrian President Assad expelled foreign journalists from the country to control media coverage of the events and their use of the internet[262]. The various internet providers in Syria operate under the government-owned Syrian Telecommunications Establishment (STE). STE, established in 1975, is central to Syria's cyber domain, providing global connectivity and regulating the flow of informa-

257 **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*. May 2017. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf.

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

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

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

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

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

tion. In addition, on numerous occasions, the Syrian Government blocked the internet and mobile phones for several days to prevent, among other things, protesters from posting videos, images or comments about the events on social media[263].

"It is against this backdrop of systematic rights violations that the new Syrian Cybersecurity Law was introduced in April 2022, which has become a de facto part of the repressive legal tactics imposed by the Syrian regime to criminalise freedom of expression and the free flow of information under the pretext of combating cybercrime."

A decade after Assad cracked down on Syrian demonstrations, the regime continues to consolidate its power by criminalising freedom of expression and shrinking civic spaces to repress any form of dissent or opposition. It is against this backdrop of systematic rights violations that the new Syrian Cybersecurity Law[264], was introduced in April 2022, which has become a de facto part of the repressive legal tactics imposed by the Syrian regime to criminalise freedom of expression and the free flow of information under the pretext of combating cybercrime.

263 **Khazan, O.** *Syria Internet outage: How it might have happened and what it means.* The Washington Post, 30 November 2022.
Available at: https://www.washingtonpost.com/news/worldviews/wp/2012/11/30/syria-internet-outage-how-it-happened/

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

1. THE REPRESSION OF POLITICAL DISSENT THROUGH AN ARMY OF BOTS[265]

Freedom of expression is subject to strict control throughout Syria. The regime has recently stepped up its already strict legislation with the adoption in April 2022 of a new Cybercrime Decree-Law[266], which imposes harsh penalties for any online activity that undermines the 'prestige of the state' or 'national unity', among other vague provisions. One of the critical points of this new Law is the control it seeks to apply to what is described as fake news[267] that may undermine the state's prestige or harm national unity. This offence carries a prison sentence of up to 5 years and heavy financial penalties. According to the Syrian Network for Human Rights (SNHR), the consequences of enacting this law have been dire for the civilian population, especially for groups of activists, human rights defenders and opponents of the regime. At least one person has died because of torture, and 146 people have been arbitrarily arrested under the new legal framework[268].

"The SNHR published a report last June 2024 analysing another recent law on establishing a Ministry of Media. According to the SNHR, this law is an instrument to consolidate the regime's control over media content, impose more censorship against the private press and publications entering the country, and impose more restrictions on television production."

The SNHR published a report last June 2024 analysing another recent law on establishing a Ministry of Media[269]. According to the SNHR, this law is an instrument to consolidate the regime's control over media content, impose more censorship against the private press and publications entering the country, and impose more restrictions on television production. In this regard, between March 2011 and May 2024, SNHR documented the murder of 717 journalists[270].

265 See glossary.

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

267 See glossary.

268 **Syrian Network for Human Rights.** "Report." 2022. Available at: https://snhr.org/wp-content/uploads/2023/08/R230812E.pdf

269 **SNHR.** "The 19/2024 Law. 2024." Available at: 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/

270 **SNHR.** *World Press Freedom Day.* 2024 Available at: https://snhr.org/wp-content/uploads/2024/05/S240419E.pdf

Before the enactment of this law, several hacker groups provided digital support to the Assad regime throughout the conflict. In this regard 2016, research was published on Group 5[271], a pro-Iranian hacker collective that supported the Assad regime. The hacker group set up websites with names such as AssadCrimes as part of their elaborate computer engineering schemes to lure opposition members and human rights defenders who could access all the information on their devices by clicking on the link.

Another hacker group that has supported Assad is the Syrian Electronic Army (SEA)[272]. The SEA operates with the support of the regime and uses DDoS attacks[273], phishing scams[274] and other tricks to surveill human rights defenders and opponents of the regime, as well as critical media. A 2013 investigation showed that the domain name of the group's website was registered in May 2011 by the Syrian Computer Society (SCS), an organization that was led by Syrian President Bashar al-Assad in 1995 before he assumed the presidency. This organisation was run by Syrian President Bashar al-Assad in 1995 before he assumed the presidency[275]. Within this group was a sub-group called The Syrian Malware Team (SMT) that used RAT (Remote Access Tool) technology to penetrate mobile devices and access all their information[276]. Even so, it is unclear whether the members of these groups have a direct connection to the Syrian Government or if they are simply a group of pro-Assad hackers.

271 **The Citizen Lab**. Group 5, Syria and the Iranian connection. 2016. Available at: https://citizenlab.ca/2016/08/group5-syria/

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

273 See glossary.

274 See glossary.

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

276 **Prince, B.** Syrian Malware Team uses Blackworm RAT in attacks. *Security Week*. 1 September 2014. Available at: https://www.securityweek.com/syrian-malware-team-uses-blackworm-rat-attacks/

2. DIGITAL CENSORSHIP AND CONTROL OF TELECOMMUNICATIONS

The Syrian Ggvernment launched its first nationwide network monitoring system in 1999. The system, commissioned by the Syrian Telecommunications Establishment was designed to monitor mobiles, fixed-line phones and the internet. Today, cyber-attacks are common, and internet monitoring is used as a weapon of war: intentional blackouts, used to temporarily disable communication networks set up by anti-regime groups, are frequent.

"Today, cyber-attacks are common, and internet monitoring is used as a weapon of war: intentional blackouts, used to temporarily disable communication networks set up by anti-regime groups, are frequent."

In the immediate aftermath of the 2011 uprising, the Syrian regime shut down all internet access in eastern Syria, and intermittent blackouts followed, which have continued throughout the conflict, as well as completely restricting content on websites covering topics deemed sensitive by the regime[277].

A few years before the Arab uprisings, the Syrian Government built communications monitoring systems through various projects in which the knowledge and experience of companies from the global North was essential. In this sense, companies such as VASTech (South Africa) and AGT (United Arab Emirates - Germany) contributed significantly to Syria's repressive surveillance state by offering solutions for the control, surveillance and censorship of networks[278]. During the beginning of the Syrian conflict, the government used telecommunications monitoring devices from Blue Coat Systems, a US-based company, for network filtering, censorship and surveillance. Despite US sanctions prohibiting sales to Syria, these devices were shipped to a distributor in Dubai and were subsequently shipped to Syria[279].

Other Western companies established links with the Assad regime by distributing digital surveillance technology. One such company is Italy's Area SpA[280], which sells monitoring systems capable of capturing internet traffic, intercepting conversations, and tracking

277 **Le VPN.** *Internet Censorship in Syria.*
Available at: https://www.le-vpn.com/internet-censorship-syria/

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

279 **The Citizen Lab.** *Behind Blue Coat.* 2011.
Available at: https://citizenlab.ca/2011/11/behind-blue-coat/

280 **Privacy International.** *Building Syria's Surveillance State.* 2016.
Available at: https://privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf

targets via GPS. It has won a government contract in Syria and Egypt[281]. The Italian company has reportedly begun installing network monitoring systems that would allow the Syrian Government to intercept, scan, and catalogue virtually all emails flowing through the country, as well as track targets and map the electronic contact networks of the Syrian population[282].

One of the companies that also facilitated the implementation of a digital surveillance structure in Syria is the German company Utimaco[283]. According to information from the European Centre for Constitutional and Human Rights (ECCHR), Utimaco participated with Area SpA in a surveillance system run by Syrian Telecom[284]. ECCHR filed a criminal complaint with the German Federal Prosecutor's Office in January 2018, in which the company was named for alleged complicity in crimes against humanity and war crimes. The French company Qosmos was also denounced before a French court by civil society organisations accusing it of supplying the Syrian Government with Deep Packet Inspection (DPI) software[285] that allowed the regime to track human rights defenders[286], dissidents and opposition members, some of whom ended up being tortured or executed after the initial uprising against the regime began in 2011[287].

In this sense, members of Syrian civil society understand their communications are being monitored and take measures in this regard. According to Abdulaziz Ramadan[288], executive director of DOZ e.V.[289], "We agreed on certain levels of security in how we share

281 **Vice.** Italian police raid SpA company headquarters. 2016. Available at: https://www.vice.com/en/article/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria/

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

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

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

285 See glossary.

286 **Corpwatch.** French Tribunal investigates Qosmos. 2015. Available at: https://www.corpwatch.org/article/french-tribunal-investigates-qosmos-over-surveillance-software-use-syria

287 **International Federation for Human Rights**. "Qosmos, the subject of a judicial investigation" 2014. Available at: https://www.fidh.org/es/region/europa-y-asia-central/francia/15435-francia-qosmos-objeto-de-una-investigacion-judicial-por-complicidad-en

288 Abdulaziz Ramadan, interview conducted as part of The Nonviolence Factory, November 2023. NOVACT team, SUDS, IRIDIA and ODHE.

289 Syrian civil society organisation based in Germany.

information on platforms like WhatsApp. "We have to think of new tools that allow us not to feel threatened and to exercise our fundamental right to freedom of expression".

3. MASS SURVEILLANCE AND CONTROL OF DIASPORA ACTIVISM VIA DIPLOMATIC MISSIONS

After the systematic repression during the Arab Spring and even more so during the Syrian war, thousands of human rights defenders fled the country. However, the Syrian regime continued the persecution beyond its borders[290]. An investigation by the Syrian Justice and Accountability Centre (SJAC) uncovered documents proving that overseas surveillance of Syrian civil society was systematically carried out across the regime's network of diplomatic missions[291]. Between 2013 and 2015, SJAC obtained access to approximately 483,000 pages of classified documents from abandoned Syrian state facilities. Through this documentation, SJAC discovered that surveillance of Syrian civil society was occurring in places as disparate as Belarus, Belgium, Cyprus, Egypt, France, Greece, Iraq, Iraq, Japan, Jordan, Lebanon, Russia, Saudi Arabia, Spain, Turkey, Ukraine, the UK, the UK and Yemen. Various intelligence agencies issued These documents between 2009 and 2012 under the Ministry of Interior and Defence. These practices of surveillance and control of Syrian civil society have also occurred in Spain, where groups of opponents of the Syrian regime protested in front of the Syrian embassy in Madrid on certain occasions.

"Un investigation by the Syrian Justice and Accountability Centre (SJAC) uncovered documents proving that overseas surveillance of Syrian civil society was systematically carried out across the regime's network of diplomatic missions."

According to information obtained by Amnesty International[292], the same embassy staff where the protests occurred were photographing and videotaping the participants

290 **Amnesty International.** *The Long Hand of the Mukhabaraat.* 2021.
Available at: https://www.amnesty.org/es/wp-content/uploads/sites/4/2021/07/mde240572011es.pdf

291 **SJAC.** Walls have ears. 2022.
Available at: https://syriaaccountability.org/content/files/2022/04/Walls-Have-Ears-English.pdf

292 **Amnesty International.** *Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home.* 2021.
Available at: https://www.amnesty.org/en/documents/mde24/057/2011/en/

to identify them. This material was then sent to the Mukhabarat[293] (Syrian intelligence service), and from there, each participant was identified, and action was taken against them and their families. Some of the consequences faced by those participating in these protests were the obstruction of administrative procedures to be carried out at the embassy[294]. At the same time, these legitimate protest practices became the perfect excuse for the Syrian regime to intimidate, threaten, arrest and even beat relatives and loved ones that the Syrian opposition community abroad still had in the country[295].

293 Mukhabarat, Arabic for intelligence, is a general term for intelligence agencies, in the Syrian case, General Intelligence (also known as State Security), Military Intelligence, Air Force Intelligence and Political Security. Available at: https://www.amnesty.org/en/documents/mde24/057/2011/en/.

294 **Amnesty International.** Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home. Índice MDE 24/057/2011, 3 October 2011.
Available at: https://www.amnesty.org/en/documents/mde24/057/2011/en/.

295 **Amnesty International.** *Syria: The long reach of the Mukhabaraat: Violence and harassment against Syrians abroad and their relatives back home*. 2011.
Available at: https://www.amnesty.org/en/documents/mde24/057/2011/en/

4. CONTROL OVER THE KURDISH COMMUNITY IN NORTH-EASTERN SYRIA

In 2022, SJAC published a report [296], after analysing sensitive documentation abandoned by the Syrian Government that are direct evidence of persecution against the Kurdish population. SJAC identified a total of 349 pages mentioning Kurdish individuals or activities, reflecting systematic repressive practices that violate human rights. Some of the measures used to persecute the Kurdish community that have been uncovered through SJAC's research are the following[297]:

- Violation of freedom of assembly and expression: Several pages invited the Syrian security apparatus to disrupt planned protests directly and to require further permits specifically for Kurdish groups to gather publicly.

- Violation of cultural rights: Two of the pages analysed conveyed fears that the expression of Kurdish culture and language threatened Syrian unity. In response to the increase in Kurdish political activities, one page described the government's plan to criminalise all Kurdish "nationalist" activities.

- Monitoring Kurdish property and economy: The documents also indicated fears about Kurdish access to land and wealth. Some pages recommended that municipalities require permits before they buy or sell land, that the Kurdish community's buying patterns be closely monitored and that the Kurdish community be punished for engaging in unauthorised real estate transactions.

- Dilute ethnic composition in Kurdish areas: One page invited Syrian state forces to put pressure on Arab tribes to move to the province of Hassakeh, ostensibly to dilute the Kurdish majority. In contrast, another page specifically recommended preventing Kurds from being the majority ethnic group in any region.

- Persuasion and intimidation of Kurdish leaders: The documents specifically ordered that Kurdish leaders be co-opted and that measures be taken to encourage Kurdish individuals to identify more as Syrian through methods of persuasion and intimidation to lure and threaten Kurdish leaders into aligning with the government.

296 **SJAC.** "Walls Have Ears." 2022.
Available at: https://syriaaccountability.org/content/files/2022/04/Walls-Have-Ears-English.pdf.

297 Ibid.

"since at least 2019, there have been various digital espionage campaigns targeting the Kurdish community on the internet."

"through fake Facebook profiles inviting people to download Android apps a Trojan virus with remote access was activated, allowing access to call logs, consulting and exporting files and taking photographs, among other functions."

- In addition, since at least 2019, there have been various digital espionage campaigns targeting the Kurdish community on the internet. In this regard, the cybersecurity company ESET and the Chinese intelligence centre QiAnXin Threat Intelligence Center discovered in 2020[298] that through fake Facebook profiles inviting people to download Android apps[299], a Trojan virus with remote access[300] was activated, allowing access to call logs, consulting and exporting files and taking photographs, among other functions.

298 **Stone, J.** "Spyware APP Designed to Monitor Kurdish." CyberScoop. 8 September 2021. Available at: https://cyberscoop.com/spyware-kurds-eset-bladehawk-iran/.

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

300 See glossary.

VII

TESTED IN SURVEILLANCE: PALESTINE AS A TESTING GROUND FOR THE STATE OF ISRAEL

Israeli military surveillance of the Palestinian people has a long history dating back to the founding of the State of Israel on Palestinian land in 1948 when 750,000 Palestinians were expelled from their homes, and Israel subjected those who remained to military rule marked by widespread surveillance[301]. It is against this backdrop of systematic violations that cybersecurity companies are part of a growing surveillance network that is reinforcing the Israeli Government's control over the Palestinian population and helping to maintain Israel's apartheid system[302].

The freedom to develop and test all kinds of weapons and security technology on the Palestinian population has allowed Israel to emerge as a world leader in surveillance technology at the beginning of the 21st century, a trend that has continued over time and which the current genocide in Gaza does not seem to affect[303]. In this regard, the Israeli Defence Forces (IDF) are the world's leading incubator of cybersecurity startups. The military service in general, and specifically the Israeli Army's Intelligence and Cybersecurity Unit 8200, serve as genuine professional experiences for young military personnel before they join the private cybersecurity sector[304]. It is unsurprising that a 2018 study cited by the Israeli daily Haaretz estimated that 80% of the 2,300 people who founded Israel's 700 cybersecurity companies were members of this Israeli Army Intelligence Unit[305].

"The freedom to develop and test all kinds of weapons and security technology on the Palestinian population has allowed Israel to emerge as a world leader in surveillance technology at the beginning of the 21st century, a trend that has continued over time and which the current genocide in Gaza does not seem to affect."

During the Arab uprisings, platforms such as Facebook, Instagram and TikTok were integral to the widespread protests across the Mashreq region, including Palestine. In this sense, the Israeli state implemented tight control of social media, which became a crucial element in the surveillance and subsequent repression of the Palestinian population[306].

---

301 **Institute for Middle East Understanding.** "Quick facts: Palestinian Refugees" 19 June 2024. Available at: https://imeu.org/article/quick-facts-palestinian-refugees

302 **Office of the United Nations High Commissioner for Human Rights (OHCHR).** *Israel's 55-year occupation of Palestinian Territory is apartheid: UN Human Rights Expert.* 22 March 2022. Available at: https://www.ohchr.org/en/press-releases/2022/03/israels-55-year-occupation-palestinian-territory-apartheid-un-human-rights.

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

304 **Daza, F.** *Invisible Walls of Occupation.* Novact. 2023. Available at: https://novact.org/wp-content/uploads/2023/10/Informe_Muros-invisibles_ocupacion.pdf.

305 **Transnational Institute.** *Israel: Model Coercive State.* 13 July 2021. Available at: https://www.tni.org/es/art%C3%ADculo/israel-modelo-de-estado-coercitivo.

306 **7amleh.** Israel's Surveillance Industry and Human Rights. December 2023. Available at: https://7amleh.org/storage/Israel%E2%80%99s%20Surveillance%20Industry%20english4.pdf

Later, within the framework of COVID-19, Israel implemented a series of legal measures that justified the expansion of surveillance systems and control technologies[307]. In this sense, the COVID-19 pandemic contributed to normalising and legitimising abuses of power and human rights violations committed by Israeli state security forces in collusion with cybersecurity companies developing and implementing these technologies[308]. One such company is NSO Group, which, in March 2020, launched a contact-tracking software called Fleming[309]. More recently (just months before the invasion of Gaza), the State of Israel passed a law known by the opposition as "Big Brother in Public Spaces", which promotes and regulates the use of biometric systems in public space by the Israeli police. The bill has far-reaching implications for the right to privacy. The intended system would allow the processing of photographs of individuals for comparison in a database[310] [311].

1. GENOCIDE AND THE USE OF ARTIFICIAL INTELLIGENCE

Israel has maintained a blockade of the Gaza Strip by land, sea and air for 17 years. In October 2023, Israel launched a new invasion of the territory, beginning the ongoing genocide of the Palestinian population. In parallel, the Israeli army and armed settlers have launched a campaign of systematic attacks against the West Bank population. These attacks have led to an escalation of control and surveillance practices over the Palestinian population. What is new in this current wave of violence and repression of the Palestinian population is the use of artificial intelligence (AI) tools.

307 **Nature.** *Mass Surveillance technologies to fight coronavirus spread: the case of Israel.* 26 May 2020.
Available at:
https://www.researchgate.net/publication/341646871_Mass-surveillance_technologies_to_fight_coronavirus_spread_the_case_of_Israel

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

309 **Forensic Architecture.** NSO's Group breach of private data with "Fleming". 30 December 2020.
Available at:
https://forensic-architecture.org/investigation/nso-groups-breach-of-private-data-with-fleming-a-COVID-19-contact-tracing-software

310 **Public Space Surveillance Law (Hebrew).**
Available at: https://www.law.co.il/media/computer-law/police_ordinance_amendment_bill2023.pdf

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

"What is new in this current wave of violence and repression of the Palestinian population is the use of artificial intelligence (AI) tools."

In this regard, the Israeli military has developed an AI-based programme[312] called "Lavender" and "Gospel[313]. According to officials from Israeli intelligence units, who have been involved first-hand in the use of AI in Gaza, Lavender has played a central role in the shelling of Palestinian civilian populations, especially during the early stages of the war[314]. These automated human targeting and infrastructure targeting systems, such as Lavender and Gospel, respectively, are joined by another tool called "Where is Daddy?", an AI system designed to track and target suspected Hamas militants at home with their families[315].

Other types of AI tools that have been used in attacks on the Gaza Strip include lethal autonomous weapons systems (LAWS) and semi-autonomous weapons (semi-LAWS)[316].The Israeli military has pioneered the use of remote-controlled quadcopters equipped with machine guns and missiles to monitor, control and attack people and infrastructure[317]. Israel has been ranked as the world's leading supplier of suicide drones[318]. Israel has been ranked as the world's leading supplier of suicide drones[319].

One of the companies involved in the ongoing genocide in Gaza is Israel's largest arms manufacturer, Elbit Systems, a major supplier to the Israeli military. Currently, 85% of all weapons, surveillance systems and tools used by the Israeli military have been manufactured by Elbit, including the Skylark and Hermes military drones, which form the majority of Israel's fleet of large unmanned aerial vehicles, which have been used extensively in Gaza[320]. The use of such tools often results in civilian casualties. It raises questions

312 **Yuval, A.** Lavender, The AI machine directing Israel's bombing in Gaza. *+972 Magazine*. 3 April 2024. Available at: https://www.972mag.com/lavender-ai-israeli-army-gaza/

313 **Yuval, A.** A mass assassination factory. *+972 Magazine*. 30 November 2023. Available at: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

314 **Frankel Pratt, S**. When AI decides who lives and dies. *Foreign Policy*. 2 May 2024. Available at: https://foreignpolicy.com/2024/05/02/israel-military-artificial-intelligence-targeting-hamas-gaza-deaths-lavender/

315 **Democracy Now!** Israel's AI Surveillance System for Palestinians. 5 April 2024. Available at: https://www.democracynow.org/2024/4/5/israel_ai.

316 **Access Now.** Artificial Genocidal Intelligence. 2024. Available at: https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/

317 **Technology and Innovation.** The future of defending Israel, Jaguar. 27 April 2021. Available at: https://www.idf.il/en/mini-sites/technology-and-innovation/jaguar-the-idf-s-newest-most-advanced-robot/

318 **Globes.** Israel Ranked as World's Top Supplier of Suicide Drones. 5 October 2023. Available at: https://en.globes.co.il/en/article-israel-ranked-as-worlds-top-supplier-of-suicide-drones-1001489297.

319 **The Jerusalem Post.** IAI Exhibits Upgraded HAROP Suicide Drone for Clients. 15 June 2016. Available at: https://www.jpost.com/Israel-News/IAI-exhibits-upgraded-HAROP-suicide-drone-for-clients-405266.

320 **Guerrero, M.** Israel's largest weapons manufacturer to help expand Us's virtual border wall. *TruthOut*. 24 July 2024. Available at: https://truthout.org/articles/israels-largest-weapons-manufacturer-to-help-expand-uss-virtual-border-wall

related to the violations of International Humanitarian Law (IHL), including the principle of distinction, where the requirement to distinguish between civilian and military targets must be met strictly[321].

The rising tide of violence in the West Bank and East Jerusalem and the genocide in Gaza have led to the emergence of a new trend of civil defence and resistance to the occupation[322]. Palestinian journalists, bloggers, content creators and influencers show the day-to-day human rights violations carried out by Israel in Gaza and the occupied West Bank as they see their work and their lives in danger. media workers and journalists have been among those targeted in Israel's war on Gaza[323]. By the end of September 2024, 128 journalists and media personnel had been killed in Gaza, according to the CPJ (Committee to Protect Journalists)[324]. One of the paradigmatic cases of Israeli harassment and control over journalists and influencers is that of Palestinian Motaz Azaiza[325] from Gaza, who, after more than 100 days of documenting the genocide in Gaza, had to be evacuated to Qatar for security reasons[326]. Another relevant case is that of Bisan Owda, a Palestinian journalist who recently received an award for showing the attacks and the reality of what is happening in Gaza[327].

"The rising tide of violence in the West Bank and East Jerusalem and the genocide in Gaza have led to the emergence of a new trend of civil defence and resistance to the occupation. Palestinian journalists, bloggers, content creators and influencers show the day-to-day human rights violations carried out by Israel in Gaza and the occupied West Bank as they see their work and their lives in danger."

321 **Verfassungsblog.** Gaza, Artificial Intelligene and Kill Lists. 16 May 2024.
Available at: https://verfassungsblog.de/gaza-artificial-intelligence-and-kill-lists/

322 **El Salto Diario.** Cyberactivism. 29 June 2024.
Available at: https://www.elsaltodiario.com/analisis/digitine-ciberactivismo-movimiento-pro-palestina

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

324 **Committee to protect journalists.** Journalists casualties in the Israel-Gaza War. 12 September 2024.
Available at: https://cpj.org/2024/07/journalist-casualties-in-the-israel-gaza-conflict/

325 **Journalism Festival.** *Motaz Azaiza.* Journalism Festival.
Available at: https://www.journalismfestival.com/speaker/motaz-azaiza

326 **McKernan.** Palestinian journalist leaves Gaza after 108 days chronicling war. The Guardian. 26 January 2024.
Available at:
https://www.theguardian.com/world/2024/jan/26/palestinian-journalist-motaz-azaiza-leaves-gaza-qatar

327 **Peabody Awards.** *It's Bisan from Gaza.* Peabody Awards.
Available at: https://peabodyawards.com/award-profile/its-bisan-from-gaza/

2. FACE RECOGNITION SYSTEMS[328] AND BIOMETRIC SURVEILLANCE

Israel's ground invasion of Gaza has been an opportunity to expand the biometric surveillance of Palestinian individuals already deployed in the West Bank and East Jerusalem. The New York Times reported how the Israeli military is using an extensive facial recognition system in Gaza "to conduct mass surveillance there, collecting and cataloguing the faces of Palestinians without their consent"[329]. According to this information, this system uses technology from the Israeli company Corsight and Google Photos to select faces from crowds and include them in a database. Corsight has developed an AI-based facial recognition application that is used by the Israeli army to monitor the Palestinian population in Gaza[330]. In addition, the Israeli army has also set up checkpoints along the main roads that the Palestinian population was using to flee the areas where the most intense attacks were taking place, with cameras scanning faces[331]. Google subsidiary Alphabet's technology is also being used, as the Israeli army uses the facial recognition feature of Google Photos as part of the total surveillance and control of the Palestinian population in Gaza. In addition to these services, Google has expanded its collaboration with the Israeli Ministry of Defence by providing a secure cloud space for processing and storing all data types[332].

"Israel's ground invasion of Gaza has been an opportunity to expand the biometric surveillance of Palestinian individuals already deployed in the West Bank and East Jerusalem"

The isolation of Gaza has not only taken place technologically but there have also been companies that have been generating profits year after year thanks to the construction of smart fences, i.e. fences that include motion sensors and biometric technology and separate Gaza from the State of Israel. In this sense, the company Magal Security plays a key

328 See glossary.

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

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

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

332 **Time.** Google contract shows deal with the Israel Defence Ministry. 2024. Available at: https://time.com/6966102/google-contract-israel-defense-ministry-gaza-war/

role[333]. Another context in which it is possible to collect more information, both personal and biometric, is at the military checkpoints or control posts imposed by Israel. Anyvision, rebranded in 2021 as Oosto[334], is collaborating with the Israeli military on a system installed at Israeli military checkpoints in the occupied West Bank that uses the company's facial recognition technology[335] for work permit identification. In September 2020, Anyvision completed the establishment of SightX, a project it shares with Israeli weapons manufacturer Rafael Advanced Defense Systems[336] [337]. SightX implements advanced detection and tracking technologies using artificial intelligence based on machine vision technology developed by Anyvision for military purposes[338].

333 **+972 Magazine.** Israel arms companies that will profit from the last assault in Gaza. 2022. Available at: https://www.972mag.com/israeli-arms-companies-surveillance-gaza/

334 **Who Profits.** Anyvision Factsheet. Available at: https://www.whoprofits.org/companies/company/6872/ar

335 See glossary.

336 **Business and Human Rights Resource Center.** Anyvision raises concerns. 28 September 2022. Available at: 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/

337 **Who Profits.** Israel Aerospace Industries (IAI). Available at: https://www.whoprofits.org/companies/company/6872/ar.

338 Ibid.

3. TECHNOLOGICAL REPRESSION AND CONTROL OF COMMUNICATIONS

Spying on human rights defenders is a worrying trend that directly affects the right to privacy and secrecy of communications, among others. In this regard, in November 2021, it was discovered that at least six Palestinian human rights defenders had their phones hacked through the Pegasus software[339]. Right after the infiltration of human rights defenders' devices, the Israeli Government included six Palestinian non-governmental organisations working in the West Bank on the list of terrorist organisations.

Another alarming trend documented is the arrest and interrogation of Palestinians for their activities on social media. Numerous cases have emerged in which people have been arrested for expressing their views or opinions on various digital platforms[340]. In addition to this tight control of social media, the Israeli army systematically inspects the mobile phones of Palestinians in East Jerusalem, often resulting in arbitrary arrests or harassment[341]. A Palestinian human rights defender recently interviewed at an international meeting shared that "while using my mobile phone when talking to someone close to me, I hear other people's voices; we have to adapt the language and adopt layers of encryption protection on our mobile devices"[342].

The bombings taking place during the current genocide have damaged the telecommunications infrastructure, causing total and partial blackouts in the Gaza Strip. They have also deliberately caused power outages that have further compromised the connectivity of the entire region. Since the beginning of the genocide, the Israeli authorities have used internet blackouts as a tool of collective punishment through a range of tactics, including imposing intermittent communications blackouts coinciding with intense bombings, destroying telecommunications infrastructure, cutting off traffic to internet service providers (ISPs) and blocking access to the fuel needed to power telecommunications services[343]. Taken together, these measures have kept the population of Gaza almost completely disconnected and severely isolated[344].

339 **Amnesty International.** Devices of Palestinian HHRR defenders hacked. 8 November 2021. Available at: https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

340 **Adalah**. Adalah monitorea las violencias de la guerra. 27 October 2023. Available at: https://www.adalah.org/ar/content/view/10939

341 **7amleh.** Briefing on the Palestinian Digital Rights Situation since October 7th 2023. 2023. Available at: https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

342 Palestinian human rights defender, interview conducted as part of The Nonviolence Factory, November 2023. NOVACT team, SUDS, IRIDIA and ODHE.

343 **Access Now.** Palestine Unplugged: how Israel disrupts Gaza's internet. 2024. Available at: https://www.accessnow.org/publication/palestine-unplugged/

344 **Access Now.** Shrinking democracy, growing violence. 2024. Available at: https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

Since 7 October 2023, Palestinian human rights defenders, influencers, and bloggers have faced increased online censorship. This censorship has been extreme on Meta-owned platforms[345], Facebook and Instagram[346], but also on other platforms such as X[347] (formerly Twitter) or Telegram, where human rights defenders have documented the systematic silencing of Palestinian voices through the arbitrary removal of content [348], the suspension of Palestinian accounts and restrictions on pro-Palestinian users and content.

"Since the beginning of the genocide, the Israeli authorities have used internet blackouts as a tool of collective punishment through a range of tactics, including imposing intermittent communications blackouts coinciding with intense bombings, destroying telecommunications infrastructure, cutting off traffic to internet service providers (ISPs) and blocking access to the fuel needed to power telecommunications services."

345 **Access Now.** How Meta censors Palestinian voices. 2024. Available at: https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/

346 **HRW Report.** Meta's broken promises. 2023. Available at: https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

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

348 **7Amleh.** Briefing on the Palestinian Digital Rights Situation. 2024. Available at: https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

VIII

JORDAN: DRIFTING INTO SELF-CENSORSHIP

Jordan's political landscape —considered a 'Trojan Horse' in the Mashreq[349], has significantly transformed in the last decade. This change has been mainly influenced by the Arab Spring, the ongoing COVID-19 pandemic and various subsequent socio-political developments. The Jordanian Government's increasing reliance on mass surveillance to maintain political control and law and order is central to these changes.

Jordan's political environment has been characterised by a mix of traditional monarchy and modern state structures, with King Abdullah II at the helm. The Arab Spring brought anti-government protests to Jordan[350] which the monarchy initially met with promises of reform and greater freedom. However, these promises were soon overshadowed by strict measures aimed at curbing dissent. In 2013, for example, the Jordanian Government blocked 304 news websites under a controversial publication law, a move seen as a direct attack on press freedom[351].

The General Intelligence Directorate (GID) (also known as "Mukhabarat") has played a central role in these surveillance activities, leveraging advanced technologies[352].

The introduction of the Cybercrime Law in 2015 marked a significant turning point in the government's efforts to control digital communications[353]. This law, which includes charges such as "spreading false news" and "inciting violence", has often been used to prosecute journalists and human rights defenders. This legal tool has allowed the government to exert greater control over online activities, leading to increased censorship and self-censorship among those who dare to speak out[354].

349 The notion of a 'Trojan horse' suggests that Jordan could be playing a hidden or strategic role for external interests or interests other than its perceived interests in a region characterised by political tensions. This implies that Jordan could be facilitating the entry or influence of external powers in the Middle East in a discreet manner.

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

351 **Jamal Halaby.** Jordan: 304 national news website blocked. AP News. 3 June 2013.
Available at: https://apnews.com/article/b1b0f9f29a5d4368b7a97792b76570ce

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

353 **Dentons.** *Cybercrime Law in Jordan.* 16 October 2023.
Available at: https://www.dentons.com/en/insights/alerts/2023/october/16/cybercrime-law-in-jordan

354 **Sukkeir, Yahia**. *Jordan. Global Information Society Watch.* 2014.
Available at: https://giswatch.org/en/country-report/communications-surveillance/jordan

1. INTERNET BLOCKING TO SILENCE DISSENTING VOICES AND NEUTRALISE SOCIAL MOBILISATION

In recent years, the Jordanian Government has acted forcefully to shut down independent news websites, clearly demonstrating its strategy of controlling the flow of information and cracking down on dissent. This action is mainly executed under the controversial 2013 Press and Publications Law[355], which ostensibly aims to prevent the dissemination of false information and maintain national security. However, in practice, this law has been used to suppress any form of media that does not align with the government's narrative, significantly undermining press freedom in the country. The collective persecution of independent media has profoundly impacted the media landscape in Jordan.

Through Article 37, the new Cybercrime Law allows the government to shut down and block websites and applications that do not respect the law[356]. Platforms like TikTok, Clubhouse, Facebook Live, Al-Hudood or 7iber have been temporarily blocked. According to government sources, these platforms and applications were blocked for allegedly spreading disinformation or inciting violence[357]. However, the platforms were blocked during mass mobilisations in the country, such as the teachers' strike in 2020 or the truck drivers' strike in Maan in 2022, to prevent human rights defenders from disseminating images and news about these protests[358]. In addition, Jordan is one of the region's countries with the most demand for information from prominent social media companies. Agencies such as the Jordanian Media Commission, the Telecommunications Regulatory Commission or other security agencies can shut down and temporarily suspend these websites.

Digital censorship is carried out through various strategies, including advanced internet monitoring technologies. The technology used to implement these measures includes sophisticated internet filtering systems such as DPI[359] that block specific URLs and

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

356 **Salam Freihat.** "Jordan's Cybercrime Law to Limit Investments and E-commerce," *SMEX*. 30 August 2023. Available at: https://smex.org/jordans-cybercrime-law-to-limit-investments-and-e-commerce/

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

358 **SMEX.** "Jordan: How Are Users Affected by the TikTok Ban?" *SMEX*. 25 May 2023. Available at: https://smex.org/jordan-how-are-users-affected-by-the-tiktok-ban/

359 See glossary.

content based on keywords and other indicators[360]. A US company has developed and implemented the Smart Filter programme in Jordan[361], which allows the government to filter and block online content deemed inappropriate or a threat to national security. This programme has been used to censor online content, restricting access to information and curtailing freedom of expression[362]. The use of this programme intensified significantly in the aftermath of COVID-19. In addition, ISPs must comply with government directives to block access to specific websites and monitor users' online activities, ensuring that these censorship measures are thoroughly enforced[363].

2. MASS HACKING OF INDEPENDENT JOURNALISM

Persecuting journalists and professionals who try to work outside strict government regulations is common in Jordan. The Cybercrime, Telecommunications, and Crime Prevention Law are the main tools used to criminalise these professionals. They circumvent the usual judicial procedures, allowing State Security Forces to arrest individuals without judicial supervision[364]. The Cybercrime Law, particularly Articles 15 and 17, has been a key tool to criminalise journalists and media personnel, giving the government broad discretionary powers to suppress press freedom.

Among the most relevant cases is the imprisonment of journalist Hiba Abu Taha, based on a complaint filed by the Media Commission on 13 May 2024 under Articles 15 and 17 of the Cybercrime Law. Initially, the alleged cybercrime was based on the publication of an investigative report in the Annasher media outlet describing the complicit relationship between the Jordanian and Israeli governments in the genocide in Gaza through the establishment of a land corridor between the two countries for the supply of materials to Israel[365]. However, it was later discovered that the accusation centred on another article in

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

361 Ibid. p. 9

362 Ibid. p.10.

363 **Privacy International.** "State of Privacy Jordan." 2019.
Available at: https://www.privacyinternational.org/state-privacy/1004/state-privacy-jordan

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

365 **Committee to Protect Journalists.** "Palestinian-Jordanian Journalist Hiba Abu Taha Sentenced to One Year in Prison." June 6, 2024. Available at:
https://cpj.org/2024/06/palestinian-jordanian-journalist-hiba-abu-taha-sentenced-to-one-year-in-prison

which Taha criticised the Jordanian Government for allowing Israel to use its airspace to intercept Iran's missiles[366]. Despite efforts to secure her release, Hiba is still being held in Juwaida prison[367]. Another similar case is that of a journalism student who faces imminent deportation to Syria despite being registered as an asylum seeker with UNHCR since 2013. Her arrest on 9 April 2024, while filming a demonstration, and her subsequent detention without judicial proceedings highlight the use of the Prevention of Crimes Act to circumvent standard legal procedures[368]. The case of Abdul Jabbar Zeitoun reflects the discretion of the State Security Forces. Zeitoun, a freelance photojournalist, was detained for a week in March 2024 while covering anti-war protests despite immediately identifying himself as a journalist at the time of his arrest [369].

Women journalists are particularly vulnerable, facing harassment, intimidation and persecution. One person was fined 5,000 dinars under the Cybercrime Law for allegedly spreading false news and defaming official institutions. Initially arrested in December 2023, she was released, and the fine was eventually cancelled under an amnesty law[370]. The personal and collective persecution of journalists and media outlets has created a climate of fear and repression, in which the risks of whistleblowing are high, and the avenues for doing so are increasingly limited. According to communication expert Mohammed Shamma: "Due to this climate of repression, people around me are afraid, and to avoid any attack, they self-censor, reducing their activism and activity on social networks"[371].

"Due to this climate of repression, people around me are afraid, and to avoid any attack, they self-censor, reducing their activism and activity on social networks"

Israeli company NSO Group's technology has been central to Jordan's crackdown on independent journalism. According to a report by Access Now, between 2019 and 2023, 35 human rights defenders and political leaders, 16 of whom were journalists, were

366 **Hiba Abu Tahar.** "ردود الأردن في الدفاع عن كيان الدعم," Annasher. 22 April 2024. Available at: https://annasher.com/exclusive/12857/

367 Access to unpublished manuscript. Mohammed Shamma, *Report on Journalist Detentions and media violations in Jordan*. Reporters Without Borders, Amman, 2024.

368 Ibid.

369 Ibid.

370 Ibid.

371 Mohammed Shamma, personal interview conducted by the research team, 25 June 2024.

digitally targeted with NSO Group's[372] Pegasus spyware[373]. Among those affected were two journalists from the Organized Crime and Corruption Reporting Project, the independent photojournalist and documentary filmmaker Abdul Jabbar Zeitoun, who was arrested on 21 March 2024 during anti-war protests, and the aforementioned journalist Hiba Abu Taha. According to Mohammed Shamma: "the aim is to silence voices and repress human rights defenders and journalists through laws and technologies that were used during the period of the Coronavirus"[374]. Pegasus remained a key component of Jordan's surveillance strategy after COVID-19.

3. DIGITAL VIOLENCE AGAINST HUMAN RIGHTS DEFENDERS AND LGBTIQ+ PEOPLE

The socio-political climate in Jordan has witnessed increasing repression of human rights defenders, characterised by arrests, intimidation and surveillance, all justified under broad legal frameworks such as the Penal Code, the Cybercrime Law and the 2006 Anti-Terrorism Law[375]. The LGTBIQ+ community is among the groups most affected by institutional control and repression. In the Jordanian landscape, there have been increasing arrests and intimidation of LGBTIQ+ persons also under the Penal Code and the Anti-Terrorism Law especially. Notable cases include the detention of the director of an LGBTIQ+ centre, arrested by the police, and the detention of human rights defenders on vague charges of endangering national security[376].Communication expert Yara Harare argues that the government cracks down on civil and political rights to override civic space and attack any group that seeks to transform Jordanian society. In this regard, Harare adds that the LGBTIQ+ community is being particularly repressed, causing fear and self-censorship among its activists, to the extent of not being able to mention words such as LGBTIQ+ or queer publicly[377].

372 See glossary.

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

374 Mohammed Shamma, personal interview conducted by the research team, 25 June 2024.

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

376 **William Christou,** "Jordan's Secret Police Accused of Targeting LGBTQ+ Community" *The Guardian.* 18 August 2023. sec. global development. Available at: https://www.theguardian.com/global-development/2023/aug/18/jordans-secret-police-accused-of-targeting-lgbtq-community

377 Yara Harare, personal interview conducted by the research team, 14 June 2024.

The technological infrastructure is part of a broader strategy of surveillance and control of digital communications, including surveillance of cybercafé users and mandatory SIM card registration. In this regard, regulations were introduced that oblige internet cafes to keep detailed records of users' identities, monitor activities through security cameras and record websites visited[378]. The mandatory registration of SIM cards with national identity cards or passport details, including biometric data, has facilitated widespread telecommunications surveillance[379]. This requirement has allowed authorities to track and intercept communications, restricting anonymity and freedom of expression.

This mass surveillance system directly impacts Jordan's freedom of expression and civic space. Prominent human rights defenders, such as lawyer Malik Abu Orabi, were repeatedly targeted with Pegasus spyware between August 2019 and July 2021[380]. Ahmad Al-Neimat, a human rights defender and anti-corruption activist, had his phone hacked in January 2021 and faced repeated detentions[381]. Lama Fakih, Middle East and North Africa director at Human Rights Watch, had her iPhone infected five times with Pegasus spyware between April and August 2021, and Hiba Zayadin, senior researcher at Human Rights Watch, received multiple notifications from Apple in 2023 that her phone was being attacked by government-sponsored spyware[382] [383]. This repressive environment fosters self-censorship and fear among journalists, human rights defenders and LGBTIQ+ people, undermining civil liberties and democratic values in Jordan[384]. According to Yara Harare, Jordan is a leader in covering up cases of persecution of activists: "There is an international news blackout on these cases"[385].

"Jordan is a leader in covering up cases of persecution of activists: "There is an international news blackout on these cases"."

378 **Privacy International.** *State of Privacy: Jordan.* 2019.
Available at: https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

379 Ibid.

380 **Front Line Defenders.** *Profile: Malik Abu Orabi.*
Available at: https://www.frontlinedefenders.org/en/profile/malik-abu-orabi.

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

382 See glossary.

383 **Human Rights Watch**, "Spyware Targets Human Rights Watch Staff in Jordan," *Human Rights Watch.* February 1, 2024.
Available at: https://www.hrw.org/news/2024/02/01/spyware-targets-human-rights-watch-staff-jordan.

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

385 Yara Harare, personal interview conducted by the research team, 14 June 2024.

4. SURVEILLANCE AND REPRESSION OF GENOCIDE PROTESTS IN GAZA

Censorship of military and security information in Jordan has intensified significantly since October 2023, reflecting the government's continued efforts to control information and suppress any form of dissent regarding its security operations and their implications for the ongoing Gaza conflict. The Cybercrime Law, Articles 15 and 17, and Crime Prevention Law are the primary legal tools facilitating this censorship and repression.

Israel's indiscriminate attacks on the people of Gaza provoked outrage in Jordan, leading to spontaneous mass demonstrations in front of the Israeli embassy in the Rabyeh district of Amman. Mohammed Shamma has documented, during 2024, 11 cases of obstruction of journalists, including in some cases arrests, for covering the pro-Palestinian demonstrations[386]. Relevant cases include Khair Eddine Al Jabri, who was arrested in March 2024 under the Cybercrime Law for republishing a video clip criticising the actions of police forces in the Gaza protests[387]. A photojournalist, he was detained for almost a month in March 2024 while covering protests in the Rabyeh area. Despite the prosecutor's decision to release him, the governor insisted on imprisoning him, thus betraying a punitive attitude towards reporting security-related events[388]. Finally, a filmmaker was pressured by the GID in March 2024 to sign a pledge not to participate in protests, such as pro-Palestinian protests, that pose a threat to the country's national security. These cases highlight a pattern of using legal frameworks such as the Cybercrime Law and the Crime Prevention Law to suppress dissent and police civil society[389].

For the obstruction and persecution of journalistic activity, exhaustive monitoring of social networks is used to identify digital content and control and monitor demonstrations. The Media Commission and the GID are relevant agencies in this mass surveillance. However, we don't know who is managing the capture of images through video surveillance cameras strategically placed in the protest area in Rabyeh. According to a researcher from the Jordan Open-Source Association, these cameras are different from the traffic control cameras found in Amman, which capture images managed by the Traffic Control Centre under the control of the Public Security and Civil Protection Directorate[390].

386 Mohammed Shamma, personal interview conducted by the research team, 25 June 2024.

387 Access to unpublished manuscript. Mohammed Shamma, *Report on Journalist Detentions and media violations in Jordan*, Reporters Without Borders, Amman, 2024.

388 Ibid.

389 Ibid.

390 **Yara AlRafie**, "Public Cameras/CCTV Amman", Jordan Open Source Association. 21 August 2022. Available at: https://www.josa.ngo/blog/217

IX

IRAQ: THE MILITARISATION OF DIGITAL SPACE

In October 2019, thousands of protesters took to the streets of Baghdad and other cities in the south of the country against government corruption. Despite the nonviolent character of the Tishreen social movement[391], Iraqi Security Forces and government-linked militias killed around 500 people in the first 7 months of the popular uprising[392]. The repression was also transferred to digital spaces where publications in support of the mobilisations led to arrests by agents of anti-terrorist units[393]. Since 2003, Iraq has become one of the most restrictive governments in the Mashreq region, with a legal framework that attacks civil liberties in society.

Persecution of political dissent in Iraq has been common practice since the British colonial period and the regime of Saddam Hussein. With the fall of the dictator, civic space opened, and thousands of non-governmental organisations and media were registered in the country. Between 2003 and 2019, more than 200 new radio stations were created in Iraq[394]. In parallel, Iraq's intelligence services were also modernised by the US and the UK to fight the insurgency in the country[395]. Since the defeat of Daesh (Islamic State of Iraq and Syria) in 2017, surveillance technologies have been used in other spheres of national security to defend the nation's values. In practice, this resulted in increased mass surveillance of human rights defenders and journalists in the country[396]. An estimated 1.3 million people in Iraq are at risk of digital violence, 75% of whom are women and girls[397].

391 Tishreen Movement is the name given to the social movement that emerged during the 2019-2021 Iraqi protests. The focus of the protests was Baghdad's Tahrir Square, with other protests taking place in Basra and Najaf.

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

393 **Human Rights Watch.** *"Iraq: Arrests for Voicing Protest Solidarity."* November 4, 2019.
Available at: https://www.hrw.org/news/2019/11/04/iraq-arrests-voicing-protest-solidarity

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

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

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

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

1. COUNTER-TERRORISM PRACTICES TO NEUTRALISE IRAQI POLITICAL DISSIDENCE

Iraq's national security architecture is predominantly military due to decades of fighting terrorism. In 2009, Iraqi Prime Minister Nour Al-Maliki created the Falcon Cell with the support of the CIA and British MI6 intelligence agencies: a specialised counter-terrorism intelligence unit with powers to investigate and neutralise national security threats without warrants. On the other hand, the US Government transferred technology to monitor and record phone calls and phone text messages to prevent terrorist attacks[398]. One of these espionage tools was probably the Stingray technology: simulated telecommunications antennas that intercept mobile communications and generate call and SMS monitoring systems[399]. In mid-2023, the new Prime Minister, Mohammed Shia Al-Sudani, appointed Abu Ali al-Basri, who was, until then, head of the Falcon Cell and head of the Iraqi National Security Services (INSS)[400].

The military's control of intelligence services[401] and the application of anti-terrorist laws and practices have contributed to the portrayal of political dissent as a threat to national security. The Anti-Terrorism Act 13 of 2005 includes ambiguities in its definition of a "terrorist act" as any threat to "national unity"[402]. The Government used the anti-terrorism law to monitor and arrest human rights defenders from the October 2019 mobilisations, justifying that these protests were violent and disrupted the social order of the country. For example, in the Anbar region, young defenders were arrested by the anti-terrorism services shortly after making posts on Facebook showing their support for the Tishreen movement in 2019[403].

---

398 **Radio Free Europe.** "U.S. Providing Iraq with Phone, SMS Monitoring Devices" *Radio Free Europe/Radio Liberty*. 21 August 2011. Available at:
https://www.rferl.org/a/us_providing_Iraq_with_phone_and_sms_monitoring_devices/24303623.html

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

400 **Suadad al-Salhy.** "Iraq: Sudani Shakes up Intelligence and Security Services in Political Power Play" *Middle East Eye*. 7 July 2023. Available at:
https://www.middleeasteye.net/news/iraq-sudani-shakes-intelligence-and-security-services-political-power-play

401 **Fawzi al-Zubaidi.** "Restructuring Iraqi National Security Institutions in Sudani's Government", The Washington Institute". 25 January 2023. Available at:
https://www.washingtoninstitute.org/policy-analysis/restructuring-Iraqi-national-security-institutions-sudanis-government

402 **Official Gazette of Iraq**. *Anti-Terrorism Law No. (13) of 2005*. Official Gazette of Iraq.
Available at: 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.

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

Iraqi national security services can obtain personal data and the content of calls, messages and emails from the country's leading telecommunications companies in national security cases. It is estimated that around 40 million Iraqis have mobile phone contracts, and 20 million have internet subscriptions with the country's two leading companies, Zain Iraq and Asian Cell. These companies are obliged to give out personal data such as location, messages and other communications of their users if there is judicial authorisation. The interaction of these companies with the INSS for national security purposes is widespread[404].

In this regard, a 2020 Peace and Freedom Organization report describes the increase in mass surveillance during election periods[405]. Surveillance aims to persuade and/or neutralise dissenting voices through different strategies, such as digital extortion[406] or physical violence. In the months leading up to the 2021 parliamentary elections, several human rights defenders were killed, and more than 30 journalists were arrested in Dhi-Qar province[407]. Specifically, the persecution and repression of human rights defenders in the city of Nassiriyah in Dhi-Qar were aimed at controlling and intimidating two political formations opposed to the government, such as Imtidad and al-Bait al-Watani[408]. The persecution of political dissent continues today, also in the Kurdistan Region of Iraq (KRI), with some very recent cases, such as the arrest of Shakar Star of Tiwar News by the Kurdish intelligence agency Asayish for allegedly preparing and publishing a report that was claimed to incite violence and disinformation[409].

The crackdown has also led to killings of human rights defenders[410], allegedly by armed militias linked to political parties in Iraq and the Iranian Government. These include the Popular Mobilisation Forces (PMF), predominantly Shia militias that were created to defend local communities from the threat of Da'esh. However, PMFs are now responsible for

404 **Tech 4 Peace.** "Privacy in Iraq -Case of Telecommunication Companies". 2023. Available at: https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

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

406 See glossary.

407 **Ali Al-Mikdam.** "The Ongoing Assassinations of Iraqi Activists," The Washington Institute. July 1, 2021. Available at: https://www.washingtoninstitute.org/policy-analysis/ongoing-assassinations-iraqi-activists

408 Ibid

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

410 **Ali Al-Mikdam.** "The Ongoing Assassinations of Iraqi Activists," The Washington Institute. July 1, 2021. Available at: https://www.washingtoninstitute.org/policy-analysis/ongoing-assassinations-iraqi-activists

systematic attacks on human rights defenders and vulnerable communities[411]. Although the Iraqi Government has attempted to integrate them into the State Security Forces, they continue to operate outside the law. For example, in 2020, Hisham al-Hashim, an analyst specialising in jihadism, was killed by a militant of the pro-Iranian militia Kataeb Hezbollah for his criticism of the government and non-state armed groups[412].

2. DIGITAL BLACKOUTS TO DISRUPT SOCIAL MOBILISATIONS AND SILENCE INSTITUTIONAL VIOLENCE

Iraq is one of the countries in the world that most often uses the disruption of internet access as a strategy to silence political activism[413]. Since 2019, the Government has blocked internet access on 126 occasions[414]. Many of these digital blackouts occurred during social protests. For example, during the Tishreen movement demonstrations in October 2019, the Government blocked internet access for over 50 days. In that period, 23 civilians were killed at the hands of State Security Forces and paramilitary groups such as PMF[415]. According to Hayder Hamzoz, Director of the INSM Foundation for Digital Rights, during periods of internet blocking, police and militia violence against human rights defenders increases, as images and videos of such attacks cannot be immediately disseminated[416]. There were also digital blackouts during the earthquake in Syria and Northern Iraq, which

411 **Shivan Fazil and Alaa Tartir.** "Iraq in 2023: Challenges and Prospects for Peace and Human", SIPRI. 17 May 2023. Available at:
https://www.sipri.org/commentary/topical-backgrounder/2023/Iraq-2023-c7y6allenges-and-prospects-peace-and-human-security

412 **Agence France-Presse.** "Iraq Court Sentences to Death Killer of Academic Hisham Al-Hashemi," Al-Monitor. May 7, 2023. Available at:
https://www.al-monitor.com/originals/2023/05/iraq-court-sentences-death-killer-academic-hisham-al-hashemi

413 **Access Now.** "Shrinking Democracy, Growing Violence. Internet Shutdowns in 2023,". May 2024. Available at: https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

414 **Alex McDonald.** "Iraq Had World's Largest Number of Internet Shutdowns in 2023 due to Exam Cheating," Middle East Eye. January 9, 2024. Available at:
https://www.middleeasteye.net/news/Iraq-largest-number-internet-shutdowns-2023-over-cheating

415 **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. December 17, 2020.
Available at:
https://timep.org/2020/12/17/from-free-space-to-a-tool-of-oppression-what-happened-to-the-internet-since-the-arab-spring/

416 Hayder Hamzoz, personal interview, 4 June 2024.

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

hurt the distribution of humanitarian aid[417]. International and local organisations have launched several campaigns against these practices, including #KeepItOn[418].

The Iraqi authorities first used Internet blockades in 2014 to fight Islamic State terrorism. Since then, as human rights expert Ismaeel Dawood points out, the government has been making this strategy more sophisticated by coordinating with the Kurdistan Region of Iraq (KRI) authorities and the country’s telecommunications and application service providers[419].

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

418 **Access Now.** *“Keep It On.”* Available at: https://www.accessnow.org/campaign/keepiton/

419 Ismaeel Dawood, personal interview, 20 June 2024.

3. THE CONTROL OF DIGITAL CONTENT: CENSORSHIP AND MASS SURVEILLANCE

The regulatory framework governing cybercrimes is obsolete and is used to limit freedom of expression and the right to non-discrimination. Civil Law No. 49 of 1951, the Communications Law of 2004 and Penal Code No. 11 of 1969[420] regulate Offences in digital spaces. For example, the Iraqi Penal Code, with provisions used during the British occupation, criminalises digital content that involves "public indecency" (art. 401 and 403)[421] or that seeks to "change the fundamental principles of the constitution or the basic laws of society"[422]. The KRI Government also has the "Law for the Prevention of Misuse of Telecommunications" to punish, including by imprisonment, the dissemination of threats, defamation, disinformation and insult, among others, that offend against honour or incite a moral crime[423]. In 2021, members of the Kurdish LGBTIQ+ rights organisation Rasan were arrested by the police for disseminating digital content "contrary to the morals of the nation". The authorities invoked Article 401 of the Penal Code[424]. The crackdown on Rasan culminated in May 2023 when a KRI court ordered the organisation's closure[425].

There are two governmental mechanisms for the implementation of this legal framework. On the one hand, the Communications and Media Commission (CMC), created in 2004, carries out mass surveillance and control of civil society's digital content, interacting with Iraq's large telecommunications companies[426]. In parallel, since 2009, the Ministry of Communications has signed several contracts with French companies to supply an internet monitoring system and block websites[427], probably with Safran and Thales[428]. Also,

---

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

421 Article 401 of the penal code punishes any person who commits an "indecent act" with imprisonment of up to six months or a fine, or both. Article 403 of the code stipulates that anyone who produces or publishes materials that offend against public morals or decency with the intention of exploiting or distributing such materials is punishable by imprisonment for up to two years or a fine, or both.

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

423 Ibid

424 Ibid

425 **Human Rights Watch**. *"Iraq." World Report 2024*. Available at: https://www.hrw.org/world-report/2024/country-chapters/iraq

426 **Tech 4 Peace**. "Privacy in Iraq -Case of Telecommunication Companies". 2023. Available at: https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

427 **OpenNet Initiative**. *"Profiles: Iraq."* Available at: https://opennet.net/research/profiles/iraq

428 **Tactical Report.** "Iraq: Thales, Safran and Security Systems." Available at: https://www.tacticalreport.com/daily/2635-Iraq-thales-safran-and-security-systems

during this period, the Citizen Lab research centre identified Blue Coat Systems applications in Baghdad's telecommunications networks linked to the City Telecom network, which allows mass surveillance[429].

On the other hand, in January 2023, the Ministry of Interior created the Digital Content Monitoring Committee to monitor and censor digital content that is harmful or contrary to the country's social and cultural norms[430]. To this end, this committee launched the "Balgh" ("Report" in English) platform the same year for civil society to report "social media content that violates public morals, contains negative and indecent messages and undermines social stability" in the words of the Minister of Interior[431]. In just one month, 96,000 complaints were received from civil society [432], some of which were followed by legal proceedings under Article 403 of the Penal Code. According to Amnesty International, the committee transferred 16 cases to the criminal courts in the same year[433]. Public figures, models and artists such as Assal Houssam, Hassan Sajmah, Sayyed Ali, Saealusa and Umm Fahd have been arrested and/or punished for publishing "indecent" content due to these new mechanisms[434]. At least 6 of them have been sentenced to prison terms in 2023[435] and at least one of them has been killed[436].

Current proposed laws to regulate digital spaces point to even greater restrictions on freedom of expression in Iraq. The Iraqi Government is discussing a draft of the Cybercrime Law that includes prison sentences of up to 10 years for publishing digital content that offends the country's religious and social principles[437]. The Communications and Media Commission (CMC) is also developing the Digital Content Regulation No. 1 of 2023 to

429 **Reporters Without Borders and the Citizen Lab.** *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*. 15 November 2013. Available at: https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

430 **Iraqi News Agency**. Ministry of Interior: form a committee to monitor content on social networking sites and hold their creators accountable. 16 January 2023. Available at: https://www.ina.iq/175883--.html?__cf_chl_tk=wVv0deBsEkhWjoMlC5MepZzKdePd.PmTxkLzbeEojyg-1719559517-0.0.1.1-4543

431 **Safaa Ayyad**, "Iraq's Controversial 'Ballegh' Platform for 'Combating Indecent Content,'" SMEX. 15 February 2023. Available at: https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content/

432 Hayder Hamzoz, personal interview, 4 June 2024.

433 **Amnesty International.** Iraq: Government must match rhetoric on human rights with meaningful action. 15 March 2023. Available at: https://www.amnesty.org/en/latest/news/2023/03/iraq-government-must-match-rhetoric-on-human-rights-with-meaningful-action/

434 **Ayad.** *"Iraq's Controversial 'Ballegh' Platform for Combating Indecent Content."* 2023. Available at: https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content/.

435 **Amwaj.** "Cases against Social Media Influencers Raise Concerns over Freedoms in Iraq". 10 May 2023. Available at. https://amwaj.media/article/Iraq-influencers-social-media

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

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

suppress online content and punish offences by internet users[438]. In parallel, the Access to Information and Freedom of Expression laws are being discussed, including legal ambiguities that could be used to restrict civil liberties[439]. Finally, the Electronic Media Reorganisation Law draft has also raised much criticism, mainly due to its potential negative impact on freedom of expression and the press[440].

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

Hate speech campaigns in the digital sphere are also a constant in Iraq. Political, religious and military leaders promote hate speech to exacerbate sectarian divisions and gain political influence. In 2022, a Shiite cleric and leader called on Iraqi society, through a post on the X (former Twitter) platform, to fight against the LGBTIQ+ community. This act contributed to the intensification of hate speech on social media[441]. In this line, the human rights group Iraqi Media House states that the "phenomenon of electronic armies has reached dangerous levels, issuing threats, including incitement to violence and hatred"[442]. In this line, some cases[443] show that political candidates have been subjected to digital extortion[444], hate campaigns and threats to get them to abandon their political careers[445]. In parallel, the United Nations states that, since 2016, at least 36 human rights defenders

438 **Article 19.** "Iraq: Drop draft Digital Content Legislation and Protect Free Speech Online". 16 March 2023. Available at: https://www.article19.org/resources/Iraq-drop-draft-digital-content-legislation-protect-free-speech-online/

439 **Tech 4 Peace.** "Privacy in Iraq -Case of Telecommunication Companies". 2023. 16 March 2023. Available at: https://t4p-storage.eu-central-1.linodeobjects.com/y778AhwIUwAvopYJsFmHZxsxStpSfb39zOnEXc0t.pdf

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

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

442 **The New Arab.** *Iran-backed 'electronic armies' threaten Iraqi activists, journalists.* 6 September 2019. Available at: https://www.newarab.com/news/iran-backed-electronic-armies-threaten-iraqi-activists-journalists

443 **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. Available at: https://t4p.co/article/2021-07-21-the-journalist-nour-al-jawahiri

444 See glossary.

445 **Orto, N.** *Iraq elections: Why some female candidates refused to run.* The New Arab. 8 October 2021. Available at: https://www.newarab.com/features/iraq-elections-why-some-female-candidates-refused-run

have been killed after being accused by unauthenticated accounts, bots and Telegram channels of being foreign agents or terrorists[446].

Online harassment campaigns combine doxing practices[447], publication of personal data and fake news[448] that put people in grave danger. are particularly affected by digital violence[449]. According to the United Nations Mission for Iraq (UNAMI), anonymous campaigns publicly expose women and girls who have participated in anti-government demonstrations, denouncing "immoral behaviour" through manipulated images[450]. During the October 2019 demonstrations, this digital violence caused many to stop participating in the mobilisations. A particularly relevant case was the murder in 2020 of activist Reham Yacoub following a disinformation campaign accusing her of having links with US agents[451].

LGBTIQ+ people are susceptible to online harassment campaigns by the government and militias. According to Human Rights Watch, online surveillance, harassment, and threats against LGBTIQ+ people are a growing trend in the region[452]. In April 2024, the Iraqi Federal Government passed a law that criminalises and punishes homosexual sexual relations with prison sentences of up to 15 years. In this framework, digital entrapment practices[453] occur on apps such as Grindr to force immoral behaviour, according to the law, on LGBTIQ+ people. These practices result in arbitrary arrests, torture and other degrading and inhumane treatment[454]. In addition, militias also use social media and online dating apps to extort from LGBTIQ+ persons digitally[455] [456].

---

446 **Ali Al-Mikdam.** Fikra Forum. 2021.
Available at: https://www.washingtoninstitute.org/policy-analysis/ongoing-assassinations-iraqi-activists

447 See glossary.

448 See glossary.

449 **Abdelkarim Anwar, Assia; Ali Farhan, Walaa, & Aziz, Tara.** *Digital Violence against Women in Iraq*. October 2023. Available at: https://portal.salamatmena.org/wp-content/uploads/2024/01/Iraq-DVAW-2023-EN.pdf

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

451 **Tech4Peace**, "From Invisibility to Visibility. Women's Digital Rights in Iraq," Tech 4 Peace. March 6, 2023.
Available at: https://t4p.co/blog/2023-03-06-from-invisibility-to-visibility-women-s-digital-rights-in-Iraq

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

453 See glossary.

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

455 See glossary.

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

CONCLUSIONS

There is a growing trend throughout the region towards authoritarianism and exhaustive control of the population, encouraged by the emergence of new technological tools and increasingly open and widespread online infiltration and impersonation practices. This a trend that has worsened since the start of the genocide in Gaza in October 2023, which undoubtedly hints at yet another turn of the screw in the repression of critical voices not only in the Maghreb and the Mashreq but also against activism in Western countries that denounce the international community's inaction or expresses support for the Palestinian people [1] [2].

In concrete terms, the following trends can be identified:

1. REPRESSIVE REGULATORY FRAMEWORKS

The starting point for mass surveillance in the Maghreb and Mashreq regions is the regulatory frameworks developed to control political dissent. Penal codes reminiscent of colonial periods are combined with new laws to control emerging forms of activism and social communication under the pretext of national security and the defence of the state's moral values. In this sense, we observe, on the one hand, the use of anti-terrorism laws and policies to curtail rights and broaden the assumptions under which surveillance and interception of people's communications are permitted. In all cases, terrorism has been conveniently exploited to portray political dissent as a threat to national security. And, in cases such as Tunisia, it has provided a perfect excuse to limit the mobility and movement of migrants and political and gender dissidents internally and abroad.

On the other hand, authoritarian regimes are developing new legal instruments to control content and new forms of digital organisation. The laws against cybercrime being passed in the Maghreb and Mashreq are justified to prevent 'immoral' behaviour, protect children and prevent the dissemination of fake news, among others. However, the reality is that they have been a turning point in the control of digital communications, which has led to increased censorship and self-censorship among those who dare to raise their critical voices, especially in areas such as independent journalism, human rights organisations and the LGBTIQ+ community. Far from preventing the circulation of false information, these new laws are being widely used in practically all the countries analysed to minimise or suppress press freedom and censor access to websites and media.

1 **Amnesty International.** *Europe: Authorities must protect the rights to freedom of expression and peaceful assembly ahead of Nakba Remembrance Day.* 10 May 2024.
Available at:
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.*
Available at:
https://www.ohchr.org/es/documents/thematic-reports/a79319-global-threats-freedom-expression-arising-conflict-gaza-report

This includes cases of digital blackouts, which governments decree, especially in times of social unrest and mass protests. This tactic is far from innocent after the proven influence that the internet had on the spread of unrest that led to the Arab Spring. These strategies obstruct the ability of social movements to organise and denounce human rights violations during critical events such as large mobilisations. Iraq is one of the countries leading the way in this political and digital strategy, with internet blockades hiding increases in police and militia violence during protests.

2. MASS SURVEILLANCE STRATEGIES AND TECHNOLOGIES

The intelligence agencies of the Maghreb and Mashreq governments continue to use communication interception as one of the main tools for the surveillance of journalists, human rights defenders, and civil society organisations. However, these mechanisms have been modernised with advanced technologies such as spyware[3] which penetrates mobile devices and computers to steal relevant information from WhatsApp or photographs.

The technology that makes the expansion of this dynamic possible is mainly provided by a small group of companies, including Western companies such as Hacking Team, Blue Coat and NSO Group. Through these companies, governments such as Israel, Morocco and Lebanon, among others, have developed extensive mass surveillance campaigns to monitor human rights defenders and access their personal and political information.

In parallel, the introduction of artificial intelligence in non-autonomous weapons and drones is identified as a new trend, ranging from extracting and storing sensitive population information (e.g. through facial recognition[4]) to programming bombs in the Gaza offensive to increase their lethal capacity. Drones are increasingly used to monitor mobilisations in countries such as Egypt, the Occupied Territory of Western Sahara or on the streets of East Jerusalem and the West Bank in Palestine.

3. ONLINE HARASSMENT

The Maghreb and Mashreq governments are global leaders in disinformation campaigns, often aimed at attacking the reputations of civil society organisations and human rights

3 See glossary.

4 See glossary.

defenders. These online attacks come from electronic armies[5] made up of thousands of bots, which underpin and intensify the daily harassment of critics and dissidents. These types of online harassment campaigns sometimes call for physical violence, increasing the risk to the lives and integrity of human rights defenders. Several cases of physical attacks and even murders preceded by online harassment campaigns have been reported in this document.

The internet has become a space that is as useful and liberating as it is potentially dangerous for civil society due to the tools used to monitor digital content in search of positions critical of the actions of governments or other political forces in countries. But it is not only the authorities who use the internet to track and punish the messages and publications of human rights defenders; other actors —such as police unions, para-police forces or militias— also lead, as in the case of Egypt and Iraq, these actions of tracking and harassment.

At times, this tactic even involves society as a whole. For example, in countries like Iraq and Morocco, authorities have established platforms for civil society to report offensive content or content that attacks the country's "morality." Specifically, in the first year of operation in Iraq, 96,000 reports were collected.

4. IMPACTOS DIFERENCIALES

These rights impacts do not affect everyone similarly but involve gender, sexual orientation, social class and legal status. There is a growing tendency to expose, harass and monitor those who break with traditional gender stereotypes and raise their voices to criticise the shrinking of democratic space, lack of rights or military occupation. This situation results in their subjection to specific types of violence, such as sexualised violence, misogynistic exposure on social media, publication of private information such as their contact and address (so-called "doxing"), or attacks on their honour. These specific coercive dynamics also target other vulnerable groups such as LGBTIQ+ people, who in many of the countries analysed are subjected to so-called "entrapment", i.e. ambushes through dating apps or on the street to accuse them of violating legal articles prohibiting same-sex relationships. Another part of this dynamic is the non-consensual exposure of their sexual orientation, the so-called "outing", a practice that can increase the risk of being subjected to further violence.

Repression that exploits structural gender inequalities also impacts on some men. This is the case of the Moroccan journalists referenced in the report, who were involved in judicial processes that used grave accusations, such as rape charges, to undermine the potential social support they received when persecuted for publishing reports and articles critical or uncomfortable for those in power.

5 Ver glosario.

The increasing criminalisation of migration and the dehumanisation of migrants passing through the countries of the region on their way to Europe (with the European Union outsourcing border control to these countries in exchange for economic packages) also has its technological side. In addition to being subjected to harassment and defamation through digital media and social networks, migrants are the subject of controversial technologies such as biometrics. In cases such as Lebanon, the seizure of mobile phones, computers and other means of communication in Syrian refugee camps is commonplace, accentuating the social isolation already suffered by these people.

Finally, it is important to highlight the differential impact that mass surveillance has on populations living under occupation, such as the Palestinian and Sahrawi peoples. A large part of the identified technologies are developed and tested on the Palestinian people living under Israeli military occupation. Meanwhile, Morocco has become a key actor in the development of the sector in the region. The business ecosystem benefits from the persistence of these occupations and the genocide against the Palestinian people.

There is no reason to believe that these trends towards an accelerated increase in the control and surveillance of the population will be reversed in the coming years, especially given the growing weakness of the international human rights protection system. It is, therefore, essential to generate tools of analysis and self-defence for critical voices and human rights defenders worldwide and, in this case, in the southern fringe of the Mediterranean region. This report aims to contribute to this purpose: to understand the phenomenon and its impacts on human rights defenders and to make the companies involved visible. This is the first step towards building alliances of resistance and collaboration and developing protection and advocacy strategies. These strategies should also establish control mechanisms for the companies involved and demand that governments guarantee human rights in the use of technologies.

RECOMMENDATIONS

The following recommendations emerge from the main findings of this report, as well as from the analysis of international practices, case studies and recommendations of various human rights organisations. The aim is to provide a comprehensive framework to prevent mass surveillance risks and protect democracy and civic space.

All recommendations apply to all institutions (states, regional governments, European Union, United Nations).

1. PROHIBITION AND REGULATION OF INTRUSIVE TECHNOLOGIES

- **Moratorium on the export and use of surveillance technologies:** States should immediately establish a moratorium on the sale, transfer, and use of surveillance technology. There is an urgent need to halt the activities carried out through surveillance technologies by all states and companies, until regulatory frameworks ensure the respect of human rights.
- **Total ban on biometric mass surveillance:** States should prohibit the total use, development, production, sale and export of facial recognition technologies and other forms of biometric surveillance without exception.
- **Prohibition of technologies tested in conflict contexts:** States should prohibit the use, development and export of surveillance technologies tested in armed conflict or contexts of occupation of civilian populations.
- **Prohibition of the use of high-risk technologies for fundamental rights:** States must prohibit, in all cases, automated profiling, emotion recognition, and biometric categorization in asylum procedures and migratory contexts, as well as in any process that could impact individuals' fundamental rights, such as in the context of a police investigation.
- **Prohibition of the use of spyware and protection of rights:** States must adopt new legal frameworks that address the challenges posed by spyware, including a ban on the production, export, sale, import, acquisition, transfer, maintenance and use of spyware, as it disproportionately interferes with fundamental rights and for which there are no adequate safeguards to prevent and redress harm to human rights.
- **Ensure intrusive-technology-free R&D programmes:** Institutions must ensure that R&D programmes don't collaborate with companies linked to developing surveillance technologies, including those in the military field.

2. TRANSPARENCY AND ACCOUNTABILITY IN THE PROCUREMENT AND USE OF SURVEILLANCE TECHNOLOGIES

- **Transparency and audit of public contracts:** Institutions must ensure the existence and implementation of control and auditing mechanisms for public technology procurements. Public procurement should include impact assessments on fundamental rights carried out by the service provider to avoid violations of fundamental rights before the service is launched. This assessment should include possible mitigation measures and even remedies in case of violations. Complaint mechanisms could be included for contracting authorities to effectively receive complaints related to the negative effects on human rights, linked to or caused by the service provider.

- **Transparency and risk assessment:** Institutions must conduct risk and human rights impact assessments before acquiring or implementing surveillance technologies, incorporating mechanisms for the participation of civil society, potentially affected groups, and other stakeholders with technical knowledge. Technology companies must provide transparency about their technologies, including information on the risk management they carry out, information about the data on which the technology has been trained—if it involves data training—and the data governance measures they have implemented to avoid biases. They must also allow audits of their algorithms, within a framework that ensures a sufficient level of confidentiality.

- **Accountability and Transparency in Public Procurement of Military and Surveillance Companies:** Institutions must ensure that military companies' access to public procurement is subject to strict human rights standards, excluding those involved in serious violations. They must promote compliance with international standards such as the Wassenaar Arrangement and encourage transparency in the trade of surveillance technologies.

3. PROTECTING DIGITAL RIGHTS: PRIVACY AND DATA PROTECTION

- **Personal data protection and privacy:** Institutions must ensure that the technologies used respect privacy rights and data protection.

- **Privacy protection and cybersecurity:** Legislations regulating electronic privacy must include stricter protections for the confidentiality of communications and the

right to protect connected devices. The security of such devices should be maintained throughout their entire lifespan, and mechanisms for complaints and remedies should be established in response to cybersecurity risks.

- **On commercial surveillance:** Institutions must establish clear regulations must be established to limit commercial surveillance practices and protect consumers' privacy. This includes prohibiting data collection without users' explicit consent and implementing transparency mechanisms that allow consumers to know how their data is being used. It is necessary to strengthen the legislation that establishes safeguards for State Security Forces' (FFSS) access to company data (e-evidence).

4. ACCOUNTABILITY, CIVIL SOCIETY PARTICIPATION AND ACCESS TO JUSTICE

- **Fostering public debate on digital surveillance:** Institutions must ensure civil society's participation in a meaningful and regular way in discussing the design and use of surveillance technologies and their impact on civil liberties and human rights.
- **Accountability and redress:** Institutions must remove obstacles that prevent victims of mass surveillance from accessing justice and ensure prompt, effective and transparent police and judicial investigations. Victims should have access to intercepted information and mechanisms for redress. Civil society must participate in everything related to the use of surveillance technologies, regularly and meaningfully, from the design, implementation, supervision, and control phases, as well as in public procurement processes. Transparency mechanisms and access to information about these technologies must exist, such as the availability of public registers so that the population can know where these technologies are being implemented.

5. INTERNATIONAL COOPERATION AND HARMONISATION

- **Creation of a working group on digital surveillance:** Institutions should establish specialised working groups to monitor and analyse abuses caused by digital surveillance, from the local to the global level, proposing recommendations to mitigate these abuses.
- **Extraterritoriality in legislation:** Institutions must include the extraterritoriality principle in all mass surveillance regulations.

- **Legislative reforms and civil society participation:** Institutions must reform security laws to align them with standards for the protection of individual and collective rights and ensure the participation of civil society in the legislative processes.
- **Human rights obligations:** Outsourcing surveillance powers to private companies does not exempt states and administrations from their human rights obligations.
- **Compliance with the Human Rights Council's Guiding Principles on Business and Human Rights:** Businesses should operate in a manner that respects human rights in all their activities, minimising risks of abuse. States must establish regulations and policies to ensure that technology companies comply with these principles of respect, prevention and accountability for human rights. States must include mechanisms for remedy in their regulatory frameworks, also in line with the Guiding Principles.

6. REGULATION AND OVERSIGHT OF COMPANIES DEVELOPING, INCORPORATING AND USING SURVEILLANCE TECHNOLOGY

- **Accountability and human rights due diligence:** Surveillance companies and those that collect data on a massive scale must integrate human rights due diligence at all stages of their product development and meaningfully engage civil society.
- **Audits and transparency:** Companies must conduct annual external audits to assess the impact of their products on human rights and facilitate access to monitor systemic risks.
- **Investing with respect for human rights:** Individuals and investing entities are urged to adopt ethical investment principles that prioritize respect for human rights in their decisions.

7. STRENGTHENING TECHNOLOGICAL SOVEREIGNTY

- **Interoperability and alternatives:** States must require interoperability between dominant technology platforms to ensure people can choose rights-respecting alternatives.
- **Public procurement rules:** States should establish criteria prioritising transparency and ethics in selecting suppliers that comply with human rights standards.

- **Open Source:** States should encourage open-source software to ensure auditing and public access to the tools used in data collection and analysis, promoting transparency and trust.
- **Public funding:** States should dedicate public funds to initiatives that focus on ethical data collection, prioritising projects that protect users' privacy and promote responsible use of technology.

ANNEXES

1. GLOSSARY

- **Advanced Persistent Threats (APTs)** are systematic hacking techniques that gain access to a digital system and remain there for a prolonged period for malicious purposes, such as theft of personal data.
- **DDoS attack:** A DDoS (Distributed Denial of Service) attack is a cyber-attack that seeks to disrupt a website's or online service's operation. It is achieved by overloading the server with many simultaneous access requests from multiple infected devices or bots. This massive influx of traffic can slow down the site or even temporarily stop working, preventing legitimate users from accessing it.
- **Zero-click attacks or network injections:** spyware techniques that allow a device to be infiltrated without the need for interaction by the affected user.
- **Coordinated Inauthentic Behaviour (Astroturfing):** masking the organisation and conduct of a coordinated campaign to make it appear to arise spontaneously from the population and civil society.
- **Data breach:** access and theft of sensitive or confidential information by illicit or illegal means.
- **Deep Packet Inspection (DPI):** a type of data processing used for many functions, including real-time and targeted monitoring, filtering and blocking Internet activity.
- **Doxing:** publishing a person's personal information and audiovisual documents without their consent.
- **Electronic Army:** a group of hackers who support the actions of a particular government and whose mission is to use the Internet, social networks and cyber-attacks to fight political opponents.
- **Digital entrapment:** tricking someone into committing a crime (according to the country's laws) in digital spaces.
- **Digital or cyber extortion** is a form of cybercrime in which individuals digitally blackmail organisations or individuals to get what they want. They may threaten to leak data, launch cyber-attacks, disable operations, prevent users from accessing data, or even destroy the data obtained.
- **Fake news refers** to the dissemination of false news or hoaxes to create a particular state of opinion, confusing and misinforming the audience.
- **Troll farm (or online trolling):** This can be a group of automated accounts (bots) or people paid to influence public opinion through social media on political or current affairs.

- **Malware:** any program or code designed to damage, exploit or infiltrate computer systems without the user's consent.
- **OAuth Phishing (Open Authorisation Phishing):** a form of phishing in which users are tricked into granting permissions to malicious applications that can access their account details and perform actions on their behalf.
- **Outing:** making a person's sexual or gender identity public without their consent.
- **Phishing:** This computer technique impersonates a trusted person, company, or service to deceive a victim, gain their trust, defraud them, or monitor their communications.
- **Facial recognition:** biometric identification of a person's identity from certain physical points on the face.
- **Spyware:** a type of malware that, although it may not harm the computer, stealthily monitors and spies on all actions performed through the infected computer.
- **Trojan Horse or Trojan virus:** a type of malware that hides behind another seemingly innocuous file to gain undetected access to a system. There are many types of Trojans (an example is the backdoor Trojan, which opens access to provide remote computer control).

2. DIRECTORY of mass surveillance companies operating in the Maghreb and the Mashreq

- **AGT (Advanced German Technologies)** is a Dubai-based company. It is mainly involved in the resale of digital forensic equipment and surveillance technology services. Its technology has been used in **Syria**[1].
- **Amesys (Advanced Middle East Systems)** is a French company controlled by the French company Bull. Amesys developed the Eagle System for digital mass traffic surveillance with censorship functions (via Deep Packet Inspection). In 2015, Amesys changed its name to Nexa Technologies and created a new mass surveillance system called Cerebro, which can track telecommunications in real-time. It has been used in **Morocco**[2] and **Egypt**[3].
- **Anyvision:** Israeli company specialising in facial recognition through smart cameras. The company's technology is used at Israeli military checkpoints against the population in **Palestine**[4].
- **AREA SpA:** An Italian company that, in collaboration with Utimaco and Qosmos, has participated in developing a central monitoring system led by Syrian Telecom for the control and surveillance of the **Syrian** population[5].

1 **Franceschi-Bicchierai, Lorenzo.** "European Surveillance Companies AGT and RCS Sell Syria Tools of Oppression." 12 December 2016. Available at: 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 November 2017. Available at: https://reflets.info/articles/maroc-popcorn-le-projet-qui-n-existait-pas.

3 **Tesquet, Olivier.** "Amesys: Egyptian Trials and Tribulations of a French Digital Arms Dealer." 5 July 2017. Available at: 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. Available at: 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 December 2016. Available at: https://www.vice.com/en/article/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria

- **Baykar:** Turkish company founded in 1984 and specialised in producing surveillance and reconnaissance drones. Bayraktar TB2 drones have been used in the Libyan, **Syrian** and Nagorno-Karabag conflicts. In 2021, **Morocco** used its drones for reconnaissance activities in **Western Sahara**[6].

- **Blue Bird Aero Systems:** Israeli company specialising in drone design and production since 2002. Israel Aerospace Industries owns 50% of its shares. There is currently a production plant for WanderB and ThunderB drones specialised in reconnaissance and surveillance missions in **Morocco**[7].

- **Blue Coat Systems:** US company acquired in 2016 by Symantec. Symantec was subsequently taken over by the Californian company Broadcom in 2019. The Blue Coat brand has disappeared, but Broadcom still uses its systems. Its technology was used to intercept and inspect data from telecommunications networks for mass surveillance of mobile devices, computers, social media interactions, emails and online communications. **Iraq**[8], **Lebanon**[9], **Syria**[10] and **Tunisia** acquired and used these systems[11].

- **Circles:** An Israeli cyber-surveillance company founded in 2011, NSO Group and Circles are controlled by US tech venture capital firm Francisco Partners. Their technology specialises in identifying vulnerabilities in communication networks to intercept calls and texts and monitor the locations of mobile devices, among other things. **Israel** and **Morocco**[12] have reportedly used this technology.

- **Cognyte** is an Israeli company specialising in cybersecurity solutions. Its research technology is used to identify security threats in the analytical spheres. However, its

6 **Soriano, Ginés.** "Morocco begins to receive combat drones manufactured in Turkey". InfoDefensa, 23 September 2021. Available at: https://www.infodefensa.com/texto-diario/mostrar/3206127/marruecos-comienza-recibir-drones-combate-fabricados-turquia.

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

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

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

10 **The Citizen Lab.** "Behind Blue Coat." 2011.Available at: 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 July 2014. Available at: https://journals.openedition.org/conflits/18863

12 **Citizen Lab.** "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles." December 1, 2020. Available at: https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

software has been used in Morocco[13] [14] to create and manage fake accounts on social networks such as Facebook, Instagram, Twitter, YouTube or VKontakte.

- **Corsight AI** is an Israeli company owned by Canadian Awz. It specialises in facial recognition. Israeli intelligence services and Unit 8200 use this technology to monitor the **Palestinian** population[15].

- **Cytrox:** a company founded in 2017 and officially based in North Macedonia, but operated from Hungary and Israel, known for its malware for cyberattacks and covert surveillance. Cytrox is part of the Intellexa Consortium, a group of spyware companies. Its Cytrox Predator product has been used in **Egypt**[16] against political opponents and journalists.

- **Dahua Technologies:** a company based in Hangzhou, China, specialising in developing surveillance and security technologies. Its number plate reading, facial recognition and motion detection cameras are in the **Occupied Territory of Palestine**[17].

- **ETI:** a Danish company specialising in cybersecurity and cyber-surveillance acquired by the German multinational BAE Systems in 2011. ETI developed Evident and X-Stream software to track internet users› browsing habits and decrypt and intercept calls and emails. **Morocco**[18] has acquired this technology. The use of this technology has also been detected in **Tunisia**[19] to repress opponents during the Ben-Ali regime.

- **Gamma Group:** A British company specialising in cybersecurity and developing surveillance technology solutions. One of its main products is the FinFisher or FinSpy spyware, which can be used to infect computers and mobile devices for data theft. FinFisher technology was found in a sophisticated cyber espionage infrastructure

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

14 **Mike Dvilyanski, David Agranovich and Nathaniel Gleicher.** "Threat Report on the Surveillance-for-Hire Industry," Meta, 16 December 2021. Available at: 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 March 2024. Available at: 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 September 2023. Available at: 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. November 2018. Available at: https://www.whoprofits.org/writable/uploads/old/uploads/2018/11/surveil-final.pdf

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

19 Ibid.

called Dark Caracal, linked to the **Lebanese** intelligence services[20]. **Egypt**[21] and **Morocco**[22] también adquirieron esta tecnología para la interceptación de telecomunicaciones.

- **Guardia Systems** is a Lebanese company in the MG Holding group. It specialises in developing technological solutions in the cybersecurity sector for extractive companies, governments and critical infrastructures. In 2006, it installed video surveillance cameras in Beirut, **Lebanon**[23] with number plate reading and recording capabilities and surveillance systems in **Iraq**[24].

- **Hacking Team (HT):** a now-defunct Italian company known for developing the Remote-Control System mass surveillance software. This spyware allowed the capture of data from mobile phones, communications on platforms such as Skype, and GPS location monitoring of devices. Its technology was acquired by the intelligence services of **Morocco**[25] and **Lebanon**[26], and has been used to persecute human rights defenders and journalists.

- **Hikvision** is a leading Chinese multinational company that offers video surveillance solutions. Its motion detection and biometric recognition cameras are installed in **Tunisia**[27] and **Jerusalem**[28].

---

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

21 **Amnesty International.** "German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed," Amnesty International, 25 September 2020.
Available at: 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 October 2015.
Available at: 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.
Available at: 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 October 2023. Available at:
https://www.intelligenceonline.com/international-dealmaking/2023/10/06/lebanese-entrepreneur-ziad-monla-vies-to-fill-iraqi-defence-s-critical-communications-needs,110062357-gra.

25 **Citizen Lab.** "Backdoors Are Forever: Hacking Team and the Targeting of Dissent," Citizen Lab, 7 October 2012.
Available at: 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 July 2015.
Available at: https://smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

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

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

- **Idemia:** French multinational specialised in automated biometric identification systems. Formerly Morpho, it has been part of Advent International since 2017, a private equity fund. Its MBIS product, which allows fingerprints, palm prints, and facial features to be obtained, was recently sold to the **Tunisian** government[29] to strengthen border security.

- **Indra Sistemas:** Spanish company with public participation, specialised in technological solutions for the defence and cybersecurity sector globally and with public involvement among its shareholders. In 2019, it contributed to expanding the satellite surveillance network to control airspace in southern **Morocco** and **Western Sahara**[30], by installing advanced communications and surveillance systems.

- **Inmobiles** is a Lebanese company. This UK-based Resource Holding Group subsidiary provides biometric capture systems to register users purchasing mobile devices in **Lebanon** according to the International Mobile Equipment Identity (IMEI) registry[31].

- **IrisGuard:** This British company, founded in 2011, specialises in biometric solutions. Several investment funds, such as GrowthGate Capital, are among its owners. Its biometric identification systems register Syrian refugees seeking assistance from UN agencies in **Jordan**[32].

- **Magal Security Systems** is Israel´s leading global perimeter systems company. It was established in 1969 by the state-owned Israeli Aerospace Industries (IAI). Since then, it has provided intelligent fencing systems with motion detection sensors and modern video surveillance cameras for illegal settlements and **Israel**´s Apartheid Wall in **Palestine**[33].

- **Mer Group:** Israeli company specialising in mass surveillance systems. Its technology can be found in the Mabat 2000 project for the surveillance of the Old City of **Jerusalem** and the control of the **Palestinian** population[34].

---

29 **Actu-Maroc**, "Kaïs Saied lance un programme de sécurité numérique en Tunisie malgré la crise économique,". 1 March 2024. Available at:
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. Available at: https://www.odhe.cat/es/indra-sistemas-s-a/.

31 **SMEX.** "Ministry of Telecommunications IMEI Registration Policy Threatens Digital Privacy," 4 December 2018. Available at:
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 April 2021. Available at: https://www.accessnow.org/press-release/irisguard-refugees-jordan/

33 **Daza, Felip.** "The Globalised Walls of Occupation. La trazabilidad de los productos de Magal Security Systems en las cadenas de suministro de la ciberseguridad en Israel y Palestina". Barcelona. ODHE and Shock Monitor. 2020.
Available at: https://novact.org/wp-content/uploads/2023/10/Informe_Muros-invisibles_ocupacion.pdf

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

- **MSAB (Mycro Systemation AB)** is a Swedish technology company leading mobile data mining and analysis. The French Lebanese company Intertech supplied Morocco with this technology. Morocco could have used this technology to persecute political dissidents and human rights defenders in the absence of controls on its use (which the EU transferred for border control).

- **MTN Syria** is a mobile service provider and a subsidiary of the South African company MTN. It has supported the **Syrian** government[35] in filtering and blocking the telecommunications of its users.

- **NSO Group:** Israeli company based in Herzliya, specialising in developing spyware to monitor and intercept data from mobile devices. Its best-known product, the Pegasus spyware, is capable of stealing data from emails, calls, and images and activating the camera of mobile phones even without the need for interaction from the affected user. Pegasus has been acquired by **Morocco**, **Lebanon**, **Jordan** and **Israel** and has been used to spy on political leaders, journalists and human rights defenders. The Moroccan and Israeli authorities have also used Pegasus spyware to monitor and control the **Palestinian** and **Sahrawi** civilian population.[36].

- **Oxygen Forensics:** a computer forensics company based in Virginia, USA. One of its main technology products is Oxygen Forensic Detective, which has mobile data analysis and extraction capabilities. The Moroccan authorities gained access to this technology in 2022 through the French Lebanese company Intertech. **Morocco**[37] could have used this technology to persecute political dissidents and human rights defenders in the absence of controls on the use of this technology (which was transferred by the EU for border control).

- **Palantir Technologies:** a company founded in 2003 and based in Denver, USA, specialises in data analytics and AI software. The Israeli army uses its technology for its military operations in **Palestine**[38].

- **Qosmos:** French company that supplied the STE (**Syrian** Telecommunications Establishment[39]) with deep packet inspection (DPI) tools, completing the project in 2012.

---

35 **Digital Dominion Report.** 2021.
Available at: https://media.business-humanrights.org/media/documents/Digital-dominion-Syria-report.pdf

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

37 **Disclose.** "How the EU Supplied Morocco with Phone Hacking Spyware," Disclose, 25 July 2022. Available at: https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware.

38 **American Friends Service Committee.** "Palantir Technologies".
Available at: https://investigate.afsc.org/company/palantir-technologies

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

- **Safran group:** A French multinational created in 2005 by defence companies. Safran, along with other companies such as Motorola, Northrup Grumman, and L-1, participated in the development of the Automated Biometric Identification System (ABIS) for the registration and systematisation of biometric data of the population of **Iraq** and **Afghanistan**[40]. In 2009, the **Iraqi** Ministry of Communications[41] contracted Safran to develop an internet monitoring and website blocking system.

- **Sandvine:** A Canadian company specialising in deep packet inspection (DPI). In **Egypt**[42], this technology has shut down more than 600 critical media or human rights organisations› websites, earning it a listing with the US Treasury Department.

- **Thales Group** is a French multinational in the aerospace, defence, security, and digital identity sectors, created in 1893 with the participation of the French government. Directly or through its subsidiary Gemalto, it has provided technology for capturing biometric data in identification documents in **Lebanon**[43] and **Morocco**[44]. Contracts on surveillance systems with the *Iraqi* Ministry of Communications[45] have also been found.

- **TKH Group:** a Netherlands-based technology company specialising in developing surveillance, communications and connectivity systems. Its subsidiary, TKH Security Solutions, sells surveillance cameras under its name and the Grundig brand to the Israeli police and illegal Israeli settlements. As of 2023, several CCTV cameras from TKH Security and Grundig have been installed in police surveillance and other infrastructure in residential areas in **East Jerusalem**[46].

- **Total Secure Defence (TSA)** is a UAE-based provider of security systems and equipment. **Morocco**[47] has acquired surveillance systems and IMSI Catchers (devices

---

40 **Nina Toft Djanegara.** "Biometrics for Counter-Terrorism: Case Study of the U.S. Military in Iraq and Afghanistan," Privacy International. June 2021. Available at: 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

41 **Tactical Report.** "Iraq: Thales, Safran and Security Systems."
Available at: https://www.tacticalreport.com/daily/2635-Iraq-thales-safran-and-security-systems

42 **Peter Guest.** "U.S. Sanctions Sandvine Over Egypt's Internet Censorship," Wired, 28 February 2024. Available at: https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/

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

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

45 **Tactical Report.** "Iraq: Thales, Safran and Security Systems."
Available at: https://www.tacticalreport.com/daily/2635-Iraq-thales-safran-and-security-systems

46 **American Friends Service Committee.** "TKH". Available at: https://investigate.afsc.org/company/tkh.

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

that trick mobile devices to obtain all phone-related information) for real-time interception of telecommunications data.

- **Trovicor:** Initially created as an intelligence department of Siemens, it was acquired by an investment fund in 2009 and set up as a company based in Dubai. In 2019, it was acquired by the French company Boss Industries. Trovicor specialises in intelligence and cybersecurity services. The Ben-Ali regime acquired its systems for interception, telecommunications data analysis, and location tracking of mobile devices from **Tunisian** civil society[48].

- **Utimaco:** a cybersecurity company based in Germany and the US. In 2021, the SGT Capital fund acquired it. The Al-Assad regime in **Syria**[49], and the Ben Ali regime in **Tunisia**[50]. used its technology to suppress the Arab revolutions through a surveillance system linked to the telecommunications network. In the case of Syria[51], Utimaco also cooperated with the Italian company Area SpA and the French company Qosmos SA.

- **URS:** A US company founded in 1951, URS specialises in technical engineering and construction services. In 2014, AECOM took over URS. In 2018, URS will supply modern video surveillance camera systems with high-resolution, long-range, thermal, and motion detection to the border fence between **Tunisia**[52] and **Libya**[53].

- **VASTech:** a South African-based company which, in partnership with AGT, has provided various communications interception technologies in **Syria**[54].

---

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

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

50 **Privacy International.** "State surveillance in Tunisia." 2019.
Available at: https://www.privacyinternational.org/state-privacy/1012/state-surveillance-tunisia

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

52 **Kapitalis.** "Des Américains installent la surveillance électronique au sud de la Tunisie," 14 August 2016.
Available at:
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," February 12, 2021.
Available at: https://www.africaintelligence.com/north-africa/2021/02/12/washington-consolidates-tunisia-libya-electronic-border-surveillance-wall,109642877-art

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

- **Veridos** is a Berlin-based company that emerged from the 2014 merger of two leading German companies in security and digital identity technology, Giesecke+Devrient and Bundesdruckerei. In 2016, they started implementing a biometric recognition system for border control in Morocco[55].

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