Mapping the supply of surveillance technologies to Africa

Morocco country report

Amira Galal

DOI: 10.19088/IDS.2023.027

1. Introduction

In recent years, Morocco has invested heavily in technology and infrastructure for digital surveillance, including the implementation of various laws and regulations. While digital surveillance can be an effective tool for protecting national security, it can also raise significant concerns about privacy and civil liberties. In Morocco, the use of digital surveillance has been the subject of ongoing debate, with human rights organisations, civil society organisations (CSOs), and activists raising concerns about its impact on individual rights and freedoms.

One of the key issues surrounding Moroccan digital surveillance is a lack of transparency and accountability. Critics argue that the extent of the government's monitoring activities is not well understood and that there is a lack of a clear legal framework governing the use of digital surveillance tools. This can result in a lack of independent oversight and checks and balances, making it easier for the authorities to abuse their power and violate the privacy of citizens.

Another concern is the potential for government to use digital surveillance to target journalists, human rights activists, and political opposition. In some cases, individuals who have spoken out against the government or reported on sensitive issues have reported being targeted for surveillance and harassment. This can have a chilling effect on freedom of speech and expression as individuals may be afraid to express their opinions for fear of government retaliation.

Despite these concerns, the Moroccan government has argued that digital surveillance is necessary for national security and law enforcement purposes, and it claims that such surveillance is subject to strict regulations and oversight. For example, the government has stated that all digital surveillance activities must be authorised by a court order and that the data collected is only used for specific purposes, such as preventing terrorism or investigating serious crimes. This report will assess whether such claims are supported by evidence.

However, human rights organisations and civil society groups argue that these regulations are not always respected in practice. In some cases, it has been reported that digital surveillance has been used to target individuals without sufficient evidence or justification. Additionally, there have been instances where the authorities have refused to disclose information about their monitoring activities, making it difficult to hold them accountable for any abuses.

2. Background

Morocco is the most westerly North African country with an ethnically diverse population of some 37.6 million Arabs, Amazigh/Berbers, and Sahrawis (tribal communities concentrated in Morocco's deserts and contested Western Sahara region). Its population is almost entirely Sunni Muslim and is largely conservative and religious. Morocco is a constitutional monarchy and holds regular multiparty elections, although King Mohammed VI maintains full dominance through a combination of substantial formal powers and informal lines of influence in both state and society. The current political climate has improved since the reign of his father, King Hassan II, when Morocco was reported to have had one of the worst human rights records in Africa and the world. Nonetheless, repression of political dissidence, and torture of citizens by officials, is still commonplace (El Hamamouchi 2023).

The Western Sahara, annexed by Morocco in 1975, is a controversial topic for both human rights defenders and civilians. Since annexation, it has been the subject of one of the longest-standing conflicts in the world, that between Morocco and the indigenous Sahrawi population, which is led by the Polisario Front. The conflict has killed between 14,000 and 21,000 people. A ceasefire agreement was reached in 1991 but broke down in November 2020. Since then, Amnesty International has documented human rights violations by the Moroccan security forces against multiple Sahrawi activists and human rights defenders, including cases of torture and rape (MacDonald 2022).

The country's Amazigh account for at least 40 per cent of the population and most Moroccans have Amazigh roots. Nonetheless, most Amazigh communities are socially, economically, and politically marginalised, driving the widescale Hirak Rif protests[1] in the northern Amazigh Rif region which stemmed from inequities experienced by many Amazigh residents and their inability to obtain justice through the political system. The state cracked down hard on the protests, arresting hundreds of activists and protesters. The Euro-Mediterranean Human Rights Monitor reported in 2021 that many had been subjected in detention to violations that affected their health and they were denied necessary health care (Euro-Mediterranean Human Rights Monitor 2021).

Terrorist groups in the Sahel, particularly in the so-called 'triangle of death' (Mali, Niger, and Burkina Faso), pose a serious threat to Morocco and its

1 The Hirak Rif Movement or Rif Movement (meaning 'Movement of the Rif') was a popular mass protest movement that took place in the Berber-speaking Rif region in northern Morocco between October 2016 and June 2017. The mass protest movement was met with repression, with many violent clashes between police and protesters in various cities and towns.

porous desert borders means that outlaws can enter and exit the country with ease. Similarly, Latin American drug traffickers have increasingly used Morocco for their transnational cocaine trade, leveraging Moroccan gangs' foothold in Europe, Africa, and the Middle East.

Morocco's constitution officially guarantees freedom of expression and the right to information, and it prohibits censorship. However, journalists are routinely subjected to arrest without warrant and prolonged pre-trial detention (The Tahrir Institute 2022). Corruption, the role of Islam, the status of the Western Sahara, the security services, the handling of the Covid-19 pandemic, and crackdowns on protests are among subjects effectively banned from media coverage. As such, the country's media is heavily restricted, de facto subject to strict censorship, many civil liberties are constrained, and criticism of the king and his entourage is severely penalised (*Africa News* 2022).

In this context of political repression, Morocco's widespread use of surveillance technologies and spyware is a serious concern. Journalists, activists, and bloggers that are critical of the state are routinely subject to arrest. Vague legislation regarding freedom of expression and the lack of an independent judiciary are used as an effective deterrent to public debate and collective action.

While the country's constitution protects freedom of expression and the right to privacy, as well as having a data protection law in place (Law No. 09-08 of 2009[2]), these laws are vaguely worded and allow for surveillance in certain circumstances, with judicial approval. This proves a great challenge given the judiciary's lack of independence and accountability and lack of oversight of the intelligence services.

Issues surrounding digital surveillance and the right to privacy are obfuscated in Morocco, grounded in vague legislation, weak national institutions, and ambiguous adherence to international treaties. For instance, Article 24 of the Moroccan 2011 Constitution[3] guarantees citizens the fundamental right to privacy, stating:

> Any person has the right to the protection of their private life. The home is inviolable. Searches may only be conducted in the conditions and forms provided by the law. Private communications, under whatever form that may be, are secret. Only justice can authorise, under the conditions and following the forms provided by the law, the access to their content, their total or partial divulgation or their summons [invocation] at the demand [charge] of whosoever.

2 See **Morocco Data Protection Factsheet**.
3 See **Moroccan Constitution 2011**.

Another instance of ambiguity relates to Morocco's adoption of the International Covenant on Civil and Political Rights (ICCPR).[4] Article 17 of the ICCPR states that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. Signatories of the ICCPR are obliged to 'adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]' (United Nations 1994). However, while Morocco's constitution affirms that international treaties have primacy over national law, it also states that this is only 'within the framework of the dispositions of the Constitution and laws of the Kingdom, in respect of its immutable national identity [Islam]'.[5] This ambiguous wording renders unclear the assertion of international treaties' supremacy over national law.

Amnesty International has documented numerous cases of the state using digital surveillance to crack down on human rights defenders. The organisation found strong evidence of Moroccan authorities using the NSO Group's Pegasus spyware. Evidence shows that as many as 10,000 individuals were targeted – including its own monarch, King Mohammed VI. This is the only confirmed case of a country monitoring its own head of state – though pundits contend that including the king's phone in the spying operation merely provided a convenient alibi, intended to exonerate him should the spyware operation be uncovered.

Prominent figures abroad have also been targeted by Morocco's surveillance. France is considering criminal charges against Moroccan officials for using Pegasus spyware to monitor French journalists and President Emmanuel Macron himself (Chrisafis 2021). Algeria also broke diplomatic ties with Morocco, citing 'massive and systemic acts of espionage' (Allen and Lime 2021) that targeted key members of its government.

In 2022, Amnesty International (2022a) uncovered the use of Pegasus spyware against activists from the disputed Western Sahara region. Moroccan authorities demanded that 'Amnesty provide evidence' for its claims in March 2022 and dismissed its report as 'arbitrary accusations' (Bounani 2021). The authorities claim that they never acquired computer software to infiltrate communications devices (*The New Arab* 2022). Yet analysis of human rights defenders' mobile phones conclusively showed that spyware had been installed on their devices.

Amnesty International says targeted attacks have been ongoing since at least 2017. While NSO Group has not outright denied the use of its software to monitor human rights defenders, it issued a statement in 2019 saying that it

4 See **International Covenant on Civil and Political Rights**.
5 See **Moroccan Consitution 2011**.

would investigate the allegations. The findings of the investigation have not been released.

In 2019, Carnegie Endowment for International Peace (Feldstein 2019) reported that Morocco had been using Chinese facial recognition software for surveillance. The following year, the interior ministry reportedly made a closed call for tenders worth almost US$10m (MAD100m) to equip drones and CCTV cameras, ostensibly to limit 'delinquency' and enforce Covid-19 social distancing and mask-wearing rules (Samaro 2022).

As digital and physical attacks on journalists and human rights defenders increase, observers report that Morocco is slowly reverting from being a 'soft' authoritarian government to a full dictatorship.

3. Supply of surveillance technology

Evidence shows that Morocco has a well-equipped and diverse surveillance landscape having procured millions of dollars' worth of digital forensics, network monitoring, spyware, and telecommunications interception from countries all over the world, including Israel, Finland, Cyprus, Italy, Germany, France, and China, among others. This section documents which companies from which countries are supplying which surveillance technologies to the Moroccan government. The information is organised into five categories.

Internet interception

In 2011, the Moroccan government was found to have invested US$2.2m in Eagle System, an online surveillance system that allows it to censor and monitor internet traffic using Deep Packet Inspection. Eagle was developed by French company Amesys Bull and is capable of intercepting countrywide communications, including email, Facebook, and instant Messenger conversations. Investigations by Privacy International in 2016 (Privacy International 2016b) found evidence of Eagle being used to spy on Moroccan civil society but they were unable to directly link it to the government. However, French investigative journalism website Reflet found direct evidence of Morocco's purchase of Eagle System in the form of procurement requests and invoices (Privacy International 2019). The outlet suggested that the French government may be complicit in the sale of the software, pointing to former French President Nicolas Sarkozy's contracts with Libya to provide Eagle and the continued close relations between the Moroccan and French governments.

Morocco also purchased malware from the Italian surveillance technology firm Hacking Team to use against journalists (Privacy International 2015). In 2015, a large trove of Hacking Team's internal documents was leaked, revealing that Morocco was one of the company's clients. The Hacking Team leaks showed that the two Moroccan intelligence agencies – the High Council for National Defence (CSDN) and the Directory of Territorial Surveillance (DST) – both purchased Remote Action Trojan malware that provides the attacker with full remote control over a target's system. The report showed that CSDN first acquired the malware in 2009 and the DST obtained it in 2012. Since the 2015 leak, there have been no further reports about Morocco's use of Hacking Team and it is unclear whether the country is still a client of the company.

Hacking Team first came into the public spotlight in 2012 when its malware was used against citizen media outlet Mamfakinch (Amnesty International

2016). The outlet was attacked a couple of days after the website was awarded a Google and Global Voices Breaking Borders Award in recognition of efforts to use the internet to promote public debate and democratic values. An email received via the contact form on the organisation's website, titled 'Dénonciation', contained a link to what appeared to be a Microsoft Word document labelled '*scandale* (2).doc' along with a message asking to keep the sender's identity anonymous. Some members of the organisation tried to open the file which ultimately necessitated 'drastic measures' to clean their computers before the file was sent for analysis.

Analysis showed that the file was a type of malicious software (malware) called a Trojan horse because of its outer cover disguises and its intent to take control of the target's computer, including taking screenshots, intercepting email, recording chats, and covertly capturing data using the computer's microphone and webcam, all while bypassing virus detection (Marquis-Boire 2012). The spy tool would detect which operating system the targeted computer was running, before attempting to infect it with either a Mac or Windows version of the virus. Once installed, the Trojan tried to connect to an IP address that was traced to US-based hosting company Linode, which provides 'virtual private servers' that host files but help mask their origin. Linode says using its servers for such purposes violates its terms of service and confirmed the IP address in question was no longer active. The process is clearly designed to obscure the identity of the government conducting the spying.

Unfortunately, Mamfakinch was forced to close as staff felt that 'it didn't matter whether our machines were clean or not, or whether we used encryption or not. They proved they could do it once. It means they can do it again' (Amnesty International 2016). Three months after the malware was detected, the outlet's team of 30 dwindled to just three contributors and eventually Mamfakinch closed due to safety concerns and fears that the government would pursue its contributors.

A Citizen Lab (Marczak *et al*. 2014) report showed that the Moroccan government had also used FinFisher malware produced by the Gamma Group of companies. Morocco has been found to use Israeli Pegasus spyware to monitor local journalists, activists, government members, foreign politicians and, as described, its own king (Bachir 2021).

Mobile interception

Morocco has also been found to intercept mobile communications. Data released by the Finnish government under the Freedom of Information Act (Privacy International 2016a) showed that Finland has issued several licences to the Finnish subsidiary of the Canadian company EXFO allowing sales of

telecommunications surveillance technology to countries including Morocco. Switzerland also released a document that revealed a list of countries that bought surveillance technologies from Swiss companies. Among the purchasers of advanced surveillance technology was Morocco, which appeared to have tested mobile telecommunication interception or jamming equipment in 2013 or 2014 (Privacy International 2015).

Citizen Lab (Marczak *et al*. 2020) reported with 'high confidence' that Morocco's interior ministry was a 'likely' client of Circles Technologies from 2018. NSO Group-affiliated Circles is a company that exploits telecommunications infrastructures' weaknesses to monitor calls, texts, and locations of phones around the globe. The report said that Citizen Lab's scanning had 'identified what appeared to be a single Circles system in Morocco'.

Security and defence company Total Secure Defence (n.d.) showed on its website that it had sold Morocco the GSM/3G Interception System and the international mobile subscriber identity catcher (IMSI catcher).

Social media monitoring

Morocco's media landscape has traditionally been very restricted and social media has posed a challenge to government fears of an Arab Spring-style mobilisation online. Many activists and journalists express concerns that they may be subject to surveillance. A Human Rights Watch report (2020) highlighted a growing government crackdown on social media users in recent years. Students, activists, citizen journalists, and social media commentators who have criticised Moroccan authorities and King Mohammed VI have been arrested and charged.

Ostensibly to fight disinformation during the Covid-19 pandemic, Morocco's government council approved but then withdrew Draft Law 22-20 related to the use of social media and open broadcast networks. According to the justice ministry, the law would 'put an end to a legislative vacuum' regarding cybercrime, allow effective response to disinformation and acts which 'damage the reputation and honour of individuals',[6] and harmonise the country's legislation with the Budapest Convention on Cybercrime,[7] despite the convention not including any clauses related to freedom of expression on social media. The draft law stipulates that network providers should restrict access to and suppress online content that could pose a threat to security and public order within 24 hours.

6 See Majalat **'In Morocco, Under Pressure From Civil Society, the 'Liberticide' Bill Concerning Social Networks is Backtracking'**.
7 See **Convention on Cybercrime**.

The year 2022 saw a marked rise in the number of activists and influencers being charged and sentenced for social media content. In March, authorities arrested blogger Saida Al-Alami (Skyline 2022) over posts critical of the Moroccan government and security services. Al-Alami, a well-known activist, has been vocal in her criticism of Morocco's authorities. The Court of Appeals convicted her of 'insulting a legally regulated institution', 'insulting public officials', 'denigrating judicial decisions' and 'spreading false allegations and facts against individuals with the aim of defaming them' (*ibid.*). She was sentenced to two years' imprisonment, later extended to three. Just days after Al-Alami's arrest, blogger Rabih al-Ablaq was detained for videos he had shared on Facebook which questioned the wealth of the king and prime minister (El Hamamouchi 2022). He was imprisoned for four years for 'publicly violating the duty of reverence and respect for the King's person' (*ibid.*).

Similarly, in September 2022, Rida Benotmane was prosecuted for criticising the authorities on YouTube and Facebook (Amnesty International 2022b). He was interrogated over posts that called for a public march against abuses by security forces and YouTube videos in which he denounced the authorities for ignoring people's demands for social justice and warned against the potential use of Covid vaccine passes as a tool of repression. He was charged with 'insulting a body regulated by law', 'insulting public officials while carrying out their duties', and 'broadcasting and distributing false allegations without consent'. He was also charged with breaching emergency health laws.

Safe city/smart city

Morocco has been ramping up efforts to adopt digital technologies while investing millions of dollars in tech-based solutions. The authorities claim that they aim to promote economic growth, increase digitalisation, and strengthen the country's innovation ecosystem through the new Maroc Digital 2020 strategy and the creation of the Digital Development Agency.

The pandemic accelerated the adoption of digital surveillance technologies in Morocco (Navarro Amuedo 2020), with the government introducing broad measures to control the spread of Covid-19 using emerging digital technologies and biometric systems such as digital identity, a Covid-19 contact tracing app, vaccine passports, and widespread installation of facial recognition software into surveillance cameras and drones.

In April 2021, the Ministry of Interior reportedly distributed a non-public call for tenders (Darouiche 2021) worth around US$94m to equip drones and CCTV cameras with facial recognition systems in Casablanca to monitor citizens' movement, limit 'delinquency', and detect persons not wearing masks or observing Covid-19 social distancing measures. The biometric system

relies on centralised data centres, databases, and algorithms that analyse citizens' movement and behaviours.

Moroccan authorities placed the regulation of biometric facial recognition software in the hands of the Moroccan National Commission for the Control of Personal Data Protection (CNDP), which had announced a moratorium on its use by public or private entities. CNDP raised concerns over the technology's impact on people's privacy and human rights and announced the need for extended consultations. The moratorium lapsed and, in August 2022, Morocco started tendering for facial recognition systems for installation in the capital's Rabat-Salé Airport (Rahhali 2022), reportedly the first time the technology will used in the country.

Biometric ID

In 2022, Morocco presented and launched its first digital identification system (*Identity Review* 2022). The Moroccan digital identity cards allow holders to prove their identity as a Moroccan citizen. As stated in a *Morocco World News* report (Rahhali 2022), 'Moroccans can use their [ID cards] as proof of identity for different places. They can physically present their electronic identity card to agents of authorized institutions to scan it and prove the holder's identity.'

Table 3.1 Supply chains of surveillance technology

Contract	Description	Dirham (MAD)	US$
Internet interception			
Amesys Bull (France)	Eagle System – can intercept countrywide communications including email, Facebook, and instant Messenger conversations (Privacy International 2016b).	20m	2m
Hacking Team (Italy)	RCS – can intercept communications, log keystrokes, and remotely control a target's device. Two purchased. Since a 2015 leak, there have been no further reports about Morocco's use of Hacking Team, and it is unclear whether the country is still a client of the company (Privacy International 2015).	4m	400,000
Gamma Group (UK/ Germany)	In 2012, there were allegations that FinFisher surveillance software had been used to spy on political dissidents. There have been no recent reports of its use, and it is unclear whether the country is still using the tool (Marczak *et al*. 2014).	Unknown	Unknown
NSO Group (Israel)	In 2021, it was reported that Pegasus spyware had been used to target journalists, human rights activists, and other public figures (Amnesty International 2022a).	~ 50m	~ 5m*
Mobile interception			
Circles Technologies (Israel)	Moroccan authorities have denied using Circles technology to monitor calls, texts, and locations of phones around the globe, but a 2020 Citizen Lab report provides evidence to the contrary (Marczak et al. 2020).	~ 30m	~ 3m†
Amesys (France)	In 2012, it was reported that Moroccan authorities had acquired a GSM/3G interception system, which can intercept phone calls and text messages (Total Secure Defence n.d.).	Unknown	Unknown
Social media monitoring			
Unknown	Although specific companies or vendors providing social media surveillance technology to Morocco are unknown, there are reports of social media surveillance leading to arrest of journalists (Human Rights Watch 2019).	Unknown	Unknown
Safe cities			
No evidence of surveillance technology			
Biometric ID			
IDEMIA (France)	MorphoWave Compact used in biometric entry-exit system launched in 2018. Uses fingerprint scanners and facial recognition technology to capture and verify the identities of people entering and leaving the country (Biotime 2020).	Unknown	Unknown
	Total	104m	10.4m

Note: *Precise figure unknown but believed to be around this figure from other Pegasus supply contracts (see Ghana report). † Precise figure unknown but believed to be around this figure from other Circles supply contracts (see Nigeria report).

Source: Authors' own, created using data from above cited sources.

4. Impacts

While most of the measures detailed are promoted by the Moroccan government as having positive consequences for safety and security, they inevitably violate key human rights recognised internationally and set out by the Moroccan state itself. For instance, Article 24 of the 2011 Constitution of Morocco[8] guarantees the right to privacy.

Morocco also has a data protection law (Law No. 09-08 of 2009)[9] in place that says that the processing of personal data can only be made if the subject has unambiguously consented to the transaction of all proposed transactions relating to their personal data. Additionally, the law stipulates that personal data cannot be disclosed to third parties without prior consent. However, the law provides for exceptions and the language is again ambiguous. For example, Article 44 states that disclosure to third parties may occur without prior consent if in the 'public interest'.[10] The law does not lay out parameters for what may be considered as public interest, leaving the law subject to abuse.

Moroccan legislation tends largely to be vaguely worded (Freedom House n.d.) and may be breached if part of a criminal investigation when a judicial order is issued. Though the law identifies specific conditions under which such orders may be granted, there remain vast grey areas regarding the discretionary powers offered to judges and intelligence agencies. The lack of an independent judiciary, and the absence of public scrutiny over the work of the intelligence services, challenge democratic oversight of these operations and leave much of the country's legislation subject to manipulation. This tactic, documented by numerous NGOs and civil society members (World Bank 2003), violates Morocco's international human rights obligations, including the right to privacy, freedom of expression and association, and the right to due process and a fair trial for those accused of a crime.

8 See **Data Protection Factsheet**.
9 See **Data Protection Laws of the World: Morocco**.
10 *Ibid.*

5. Solutions

The first step to solving the problem of Moroccan digital surveillance is to understand its root causes. One of the main drivers behind digital surveillance in the country is the desire for national security. The country faces many internal and external threats that pose a risk to its stability and security. For example, Morocco faces the threat of terrorism from extremist groups, as well as threats from drug trafficking and cybercrime.

To protect its citizens, the government has implemented a surveillance system that monitors online activities. However, the government's justification for digital surveillance goes beyond the protection of national security. Morocco has a history of political repression and human rights violations, and the use of digital surveillance is seen as a tool for suppressing dissent, rights to privacy, and freedom of expression. It has led to a widespread perception among the population that the government is using digital surveillance to restrict freedom of speech and expression.

It is essential to find a balance between national security and the protection of citizens' rights. It is essential for the Moroccan government to engage in ongoing dialogue with civil society and human rights organisations, and to put in place effective oversight mechanisms and legal frameworks to ensure that digital surveillance is used in a responsible and ethical manner.

Regulation and oversight

One of the first steps in resolving the issue of digital surveillance in Morocco is to establish clear and transparent legal frameworks that govern its use. This includes clear regulations and guidelines for the government to follow when monitoring digital communications and activities, as well as clear oversight mechanisms and remedies for individuals who believe their rights have been violated. The legal framework should be guided by international human rights standards and principles, including the rights to privacy and freedom of expression. This will ensure that the use of digital surveillance is subject to appropriate checks and balances, and that individuals can challenge abuses of power. There is no single solution that will address all concerns around digital surveillance in Morocco and a multifaceted approach will certainly be needed.

Transparency and accountability

The government should engage in dialogue with citizens to build trust and confidence in digital surveillance systems to ensure transparency and accountability. This can be achieved through public consultations and

engagement with CSOs that are dedicated to protecting the rights of citizens. The government should also ensure that citizens have access to information about surveillance systems and the ways in which they are used. Additionally, there should be mechanisms in place for people to challenge and hold organisations accountable for any potential misuse of their data.

In addition to advocacy for these kinds of national reforms and establishing clear legal frameworks, human rights defenders should leverage independent means of reclaiming digital spaces without putting themselves at risk.

Privacy-focused technologies

Another important step is the development of technical solutions that protect citizens' privacy and security. This can be achieved through the use of encryption technologies, such as virtual private networks (VPNs) and secure messaging apps that help prevent unauthorised access to digital information and protect sensitive data from theft or misuse.

Awareness and education

Greater awareness and education about the issue of digital surveillance is needed so that people can understand the risks and take steps to protect themselves. This could include providing information about privacy-focused technologies, as well as tips for using the internet and social media securely and confidentially. On an international level, human rights defenders should develop comprehensive archives that catalogue surveillance cases and push for litigation against suppliers of surveillance technologies that are likely to be abused.

6. Surveillance stories

There are many cases in Morocco which illustrate how human rights have come under fire from digital surveillance in recent years.

Journalists

As far back as 2013, independent journalist Ali Anouzla was accused of 'glorifying terrorism' (Amnesty International 2013) after being subject to pervasive surveillance. A target of nationalist hacker groups, Anouzla also found numerous online recordings on social media sharing his private phone conversations. After publicly stating that this was likely linked to Morocco's intelligence service, he was sued by the government. He told Privacy International:

> *Knowing your phone conversations are constantly listened to is disturbing. It restrains my private life. For instance, even though I don't drink, I know I cannot go to a place where people drink alcohol because I could be photographed and in a Muslim country this could be used to shock people. Other than that, it never prevented me from saying and writing anything.* (Privacy International 2018: 34)

Omar Radi is an award-winning Moroccan investigative journalist and activist who worked for national and international media outlets. His work investigated links between corporate and political interests in Morocco and it touched upon questions of corruption and human rights abuses in Morocco. His phone was hacked using Pegasus spyware in June 2020 after he uncovered a scandal implicating nearly 100 public officials of illicitly acquiring residential properties on state lands at a fraction of their worth. In March 2022, he was sentenced to six years' imprisonment on charges of espionage and rape (Amnesty International 2022c).

An investigation by Amnesty International's Security Lab found that Radi's phone had been subjected to multiple network injections (Amnesty International 2020). The attacks occurred over a period when Radi was being repeatedly harassed by the Moroccan authorities, with one attack taking place just days after NSO Group pledged to stop its products being used in human rights abuses. The attacks continued until at least January 2020.

The academic

Since 2015, French-Moroccan academic and human rights defender Maati Monjib has believed he is under digital surveillance by the authorities. This has had a detrimental impact on his activism and daily life. Constantly analysing his digital communications caused great psychological harm. He told Amnesty International:

> *I need to constantly analyse the consequences of what I say and the risk that this may lead to defamatory accusations against me. This even applies to very practical things like arranging meetings or a dinner downtown.*
> (Amnesty International 2019a)

Amnesty International investigated his case and found he had been repeatedly targeted with malicious Short Message Service (SMS) messages that carried links to websites connected to NSO Group's Pegasus spyware. In 2020, Monjib was arrested in Rabat and sentenced to one year's imprisonment for 'undermining the internal security of the state' and 'defrauding' the government.

The YouTuber

In 2019, Moroccan YouTuber Mohamed Sekkaki was sentenced to four years' imprisonment and fined around US$4,000 after being found guilty of insulting King Mohammad VI, having described the king's speeches as 'useless'. He also described Moroccans as 'donkeys' as they silently watched their rights being abused. At the end of the now-removed 12-minute-long video, Sekkaki predicted his arrest (BBC News 2019).

Human rights defenders

Mahjoub Maliha, an activist supporting human rights in the longstanding Western Sahara conflict between Morocco and Sahrawi separatists was shocked to find out that Moroccan authorities had hacked his phone. He told Amnesty International that he noticed the breach when he noticed that emails from Sahrawi human rights defenders were appearing as read on his phone. Amnesty's tech team confirmed the device was infected by Pegasus.

Human rights defender Aminatou Haidar was also found to have been targeted with Pegasus spyware. Sahrawi activist group, the Nushatta Foundation, said that Morocco employed multiple techniques, including Pegasus spyware, to extract compromising information with which to discredit Sahrawi activists:

> *Pegasus allows Moroccan intelligence to access all our data, including personal information that can be used to defame us and to block connections we try to make with outside countries… We will be accused of sleeping with people because we live in a conservative society and that is a good way to discredit us.*
> (Rickett 2022)

After receiving email security alerts from Apple saying her phones may have been targeted by spyware, Haidar was referred to Amnesty International's Security Lab. Forensic analysis confirmed that her phone had been targeted by Pegasus spyware dating back to September 2018. These findings were corroborated by Citizen Lab (Amnesty International 2019b).

The lawyer

Abdessadek El Bouchataoui, a lawyer and human rights defender, was imprisoned for participating in social justice protests during the Hirak protests of 2016–17. In February 2017, Morocco sentenced him to 20 months' imprisonment for online posts in which he criticised the excessive force used by the authorities against protesters. He told Amnesty International (2019b): 'Surveillance is a type of punishment. You can't behave freely. It is part of their strategy to make you suspect you're being watched so you feel like you're under pressure all the time', adding that he had faced death threats, been followed, and that his family and associates had been harassed. He has now sought asylum in France.

References

Africa News (2022) '**Morocco: Activist Gets Four Years in Prison for Criticising King**', 1 May (accessed 1 February 2023)

Allen, N. and Lime, M.L. (2021) ***How Digital Espionage Tools Exacerbate Authoritarianism Across Africa***, 19 November, Washington DC: Brookings Institution (accessed 6 July 2023)

Amnesty International (2022a) ***Morocco/Western Sahara: Activist Targeted with Pegasus Spyware in Recent Months – New Evidence***, 9 March (accessed 25 January 2023)

Amnesty International (2022b) ***Morocco: Free Activist Rida Benotmane Immediately and Drop All Charges Against Him***, 21 September (accessed 9 February 2023)

Amnesty International (2022c) ***Morocco: Ensure Fair Appeal Trial to Journalist Omar Radi***, 2 March (accessed 10 July 2023)

Amnesty International (2020) ***Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools***, 22 June (accessed 10 July 2023)

Amnesty International (2019a) ***Morocco: Human Rights Defenders Targeted with NSO Group's Spyware***, 10 October (accessed 25 January 2023)

Amnesty International (2019b) '**Moroccan Human Rights Defenders Targeted using Malicious NSO Israeli Spyware**', *Amnesty International*, press release, 10 October (accessed 10 July 2023)

Amnesty International (2016) '**How a Hacking Campaign Helped Shut Down an Award-Winning News Site**', 9 December (accessed 9 February 2023)

Amnesty International (2013) ***Urgent Action: Journalist Charged Under Anti-Terrorism Law***, 26 September (accessed 10 July 2023)

Bachir, M. (2021) '**Pegasus: From its Own King to Algeria, The Infinite Reach of Morocco's Intelligence Services**', *Middle East Eye*, 21 July (accessed 25 January 2023)

BBC News (2019) ***Morocco YouTuber Mohamed Sekkaki Jailed for Insulting King Mohammed VI***, 27 December (accessed 10 July 2023)

Biotime (2020) ***The Kingdom of Morocco Launches a National Digital ID Platform with IDEMIA*** (accessed 10 July 2023)

Bounani, A. (2021) '**Pegasus: une affaire marocaine, vraiment?**', *Le Point Afrique*, 28 July (accessed 25 January 2023)

Chrisafis, A. (2021) '**Emmanuel Macron Identified in Leaked Pegasus Project Data**', *The Guardian*, 20 July (accessed 25 January 2023)

Darouiche, M. (2021) '**Casablanca sous l'œil des caméras et des drones**', *Hespress*, 22 April (accessed 25 January 2023)

El Hamamouchi, A. (2023) '**Human Rights Deteriorating in Morocco: Rabat's Defamation Drive**', *Qantara*, 2 February (accessed 2 February 2023)

El Hamamouchi, A. (2022) '**Escalating Repression in Morocco**', *Sada*, 12 May (accessed 9 February 2023)

Euro-Mediterranean Human Rights Monitor (2021) '**Morocco: Euro-Med Monitor Condemns the Ill-Treatment of Hirak Rif Detainees**', press release, 25 February (accessed 1 February 2023)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Working Paper, Washington DC: Carnegie Endowment for International Peace (accessed 25 January 2023)

Freedom House (n.d.) ***Freedom on the Net 2021: Morocco*** (accessed 25 January 2023)

Human Rights Watch (2020) ***Morocco: Crackdown on Social Media Critics***, 5 February (accessed 25 January 2023)

Human Rights Watch (2019) ***Morocco: Free Outspoken Journalist Jailed Over Tweet***, 28 December (accessed 10 July 2023)

Identity Review (2022) '**Moroccan Digital Identity: Expanding Accessibility. Inside Morocco's Growth and Acceleration of Digital Identification Technologies**', 20 June (accessed 10 July 2023)

MacDonald, A. (2022) '**Western Sahara: Women Activists Say They Face Rape, House Arrest and Forced Divorce**', *Middle East Eye*, 21 April (accessed 1 February 2023)

Marczak, B. ; Scott-Railton, J.; Rao, S.P.; Anstis, S. and Deibert, R. (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles***, Citizen Lab Research Report 133, Toronto: University of Toronto, (accessed 1 February 2023)

Marczak, B. ; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) **Mapping Hacking Team's 'Untraceable' Spyware**, Citizen Lab, 17 February (accessed 25 January 2023)

Marquis-Boire, M. (2012) ***Backdoors are Forever: Hacking Team and the Targeting of Dissent?***, Citizen Lab, 10 October (accessed 9 January 2023)

Navarro Amuedo, A. (2020) '**Drones with Domestic Technology to Keep the Virus at Bay in Morocco**', *Atalayar*, 8 May (accessed 25 January 2023)

Privacy International (2019) ***State of Privacy Morocco***, 26 January (accessed 25 January 2023)

Privacy International (2018) ***Their Eyes On Me: Stories of Surveillance in Morocco***, London: Privacy International (accessed 25 January 2023)

Privacy International (2016a) ***With New Spying Powers on Horizon, Surveillance Companies Descend on UK,*** 9 March (accessed 10 July 2023)

Privacy International (2016b) '**The Right to Privacy in Morocco: Human Rights Committee 116th Session**', London: Privacy International (accessed 16 August 2023)

Privacy International (2015) ***Facing the Truth: Hacking Team Leak Confirms Moroccan Government Use of Spyware***, 10 July (accessed 25 January 2023)

Rahhali, L. (2022) '**ONDA Opens Tender for New Face ID Recognition System in Rabat Airport**', *Morocco World News*, 4 August (accessed 9 February 2023)

Rickett, O. (2022) '**Pegasus Spyware: Western Sahara Activist Aminatou Haidar Targeted**', *Middle East Eye*, 9 March (accessed 10 July 2023)

Samaro, D. (2022) '**Pandemic Tech and Digital Rights in Morocco**', *Global Voices*, 30 March (accessed 25 January 2023)

Skyline (2022) '**Morocco: Skyline Condemns the Increase in the Prison Sentence Against Activist 'Saida Al-Alami' and Calls on the Authorities to Release Her Immediately and Unconditionally**', *Skyline International for Human Rights*, press release, 26 September (accessed 9 February 2023)

The New Arab (2022) '**Morocco Demands Amnesty to Provide Evidence of Pegasus Spyware Claims**', 18 March (accessed 25 January 2023)

The Tahrir Institute (2022) *Press Freedoms in Morocco*, Washington DC: Tahrir Institute for Middle East Policy

Total Secure Defence (n.d.) ***Exporting GSM/3G Interception & IMSI Catcher to Morocco*** (accessed 9 February 2023)

United Nations (1994) ***Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, HRI/GEN/1/Rev.1 at 21*** (accessed 6 July 2023)

World Bank (2003) ***Morocco: Legal and Judicial Sector Assessment***, Washington DC: World Bank (accessed 25 January 2023)