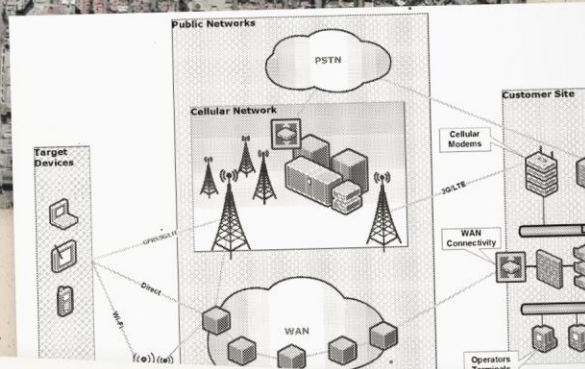


AMNESTY
INTERNATIONAL



“WE START WITH THE VERDICT”

INSIDE MOROCCO'S
SURVEILLANCE MACHINE



Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

© Amnesty International 2026

Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

For more information please visit the permissions page on our website: www.amnesty.org

Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.

First published in 2026

by Amnesty International Ltd

Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: MDE 29/1447/2026

Original language: English

amnesty.org



Cover illustration: © Rectangle / Evan Grothjan

AMNESTY
INTERNATIONAL



CONTENTS

1. EXECUTIVE SUMMARY	11
2. METHODOLOGY	18
3. BACKGROUND	21
3.1 PROSECUTIONS AND HEAVY PRISON SENTENCES FOR EXPRESSION	22
4. INSIDE PEGASUS: THE EVOLUTION OF THE WORLD'S MOST NOTORIOUS SPYWARE SYSTEM	25
4.1 THE PEGASUS INFECTION PROCESS FROM THE ATTACKER PERSPECTIVE	26
4.1.1 THE PEGASUS DASHBOARD: USERS, GROUPS, AND CASES	27
4.1.2 LAUNCHING A PEGASUS ATTACK: TARGET SELECTION, DEVICE FINGERPRINTING, AND VECTOR DELIVERY	29
4.1.3 THE PEGASUS INFECTION PROCESS	32
4.1.4 NEW MATERIAL FURTHER VALIDATES SIGNIFICANCE OF PEGASUS PROJECT LEAK	36
4.2 EVOLUTION OF PEGASUS INFECTION VECTORS	40
4.2.1 INFECTION WITH ZERO-CLICK ATTACKS	42
4.3 FORENSIC ATTRIBUTION OF ATTACKS BASED ON CUSTOMER-SPECIFIC INDICATORS OF COMPROMISE	42
4.4 HOW NEWLY DISCLOSED DOCUMENTS ENHANCE PUBLIC UNDERSTANDING OF PEGASUS SPYWARE	43
5. THE USE OF PEGASUS SPYWARE IN MOROCCO	45
5.1 HISTORY OF PEGASUS USE BY MOROCCAN AUTHORITIES	45
5.1.1 INFECTION WITH 1-CLICK LINKS	46
5.1.2 NETWORK INJECTION ATTACKS	49
5.1.3 ZERO-CLICK ATTACKS	50
5.1.4 MOROCCAN GOVERNMENT ABUSIVE USE OF PEGASUS TO TARGET HRDS	51
5.1.5 DENIAL AND BACKLASH FROM THE MOROCCAN AUTHORITIES	52
5.2 MORGAN: MOROCCO'S PEGASUS OPERATOR REVEALED	53
5.2.1 EARLY PEGASUS CUSTOMER TESTING EXPOSES THE SPYWARE OPERATORS	54
5.3 HUMAN RIGHTS DEFENDERS AMONG THE FIRST TARGETS	55
5.3.1 ADDITIONAL NSO-CONNECTED SYSTEM DEPLOYED IN MOROCCO AT THE SAME TIME AS PEGASUS SYSTEM DEPLOYMENT	56
5.4 MOROCCO'S USE OF PEGASUS SPYWARE BEYOND ITS BORDERS	58

5.4.1 TIMELINE OF MOROCCO'S SELECTION OF PEGASUS TARGETS ABROAD	59
5.5 FORENSIC ATTRIBUTION OF ATTACKS TO MOROCCO BASED ON REUSED ZERO-CLICK ATTACK EMAIL ADDRESSES	61
6. OTHER DIGITAL SURVEILLANCE TECHNOLOGIES USED IN MOROCCO TO TARGET CIVIL SOCIETY	64
6.1 HACKING TEAM RCS SPYWARE (2009–2024)	65
6.2 PHYSICAL INFECTION OF DEVICES	67
6.3 IMSI CATCHERS	72
6.4 MASS SURVEILLANCE TECHNOLOGIES	73
6.4.1 EAGLE / CEREBRO MASS INTERNET SURVEILLANCE SYSTEM	73
6.4.2 MAGAZINE: VERINT SUPPLIES LARGE SCALE INTERCEPTION SYSTEMS TO MOROCCO	74
7. UNLAWFUL SURVEILLANCE: TOOLS AND TECHNIQUES IN PRACTICE	76
7.1 TARGETING FAMILY AND NETWORKS	78
7.2 LISTENING AND WATCHING EVERYWHERE	80
7.2.1 PHONE TAPPING THROUGH TELECOM NETWORKS	80
7.2.2 AUDIO AND VIDEO RECORDING IN PUBLIC AND PRIVATE SPACES	81
7.3 HUMAN SOURCES	85
7.4 DIGITAL FORENSIC TOOLS	86
7.5 SURVEILLANCE OPERATIONS	87
8. SMEAR CAMPAIGNS	92
8.1 DEFAMATION VIA SOCIAL MEDIA	96
8.2 SMEAR CAMPAIGNS AND INTERNATIONAL HUMAN RIGHTS LAW	97
9. HUMAN IMPACTS AND CHILLING EFFECT	101
10. SURVEILLANCE - LEGAL FRAMEWORK	104
10.1 INTERNATIONAL HUMAN RIGHTS LAW AND STANDARDS ON SURVEILLANCE	104
10.2 MOROCCAN DOMESTIC SURVEILLANCE SAFEGUARDS AND PRACTICES IN LIGHT OF INTERNATIONAL HUMAN RIGHTS LAW AND STANDARDS	107
10.3 THE HUMAN RIGHTS RESPONSIBILITIES OF CORPORATE ACTORS	108
10.4 CORPORATE ACTORS' ROLE IN UNLAWFUL SURVEILLANCE IN MOROCCO	109
11. CONCLUSION AND RECOMMENDATIONS	111
11.1 TO THE MOROCCAN AUTHORITIES	112
11.2 TO ALL STATES	113
11.3 TO STATES FROM WHICH SURVEILLANCE OR OTHER PRIVACY-INVADING TECHNOLOGY IS EXPORTED, SOLD OR BROKERED	113
11.4 TO COMPANIES INVOLVED IN SUPPLYING SURVEILLANCE AND OTHER PRIVACY-INVADING TECHNOLOGY TO MOROCCO	114
11.5 TO TELECOMMUNICATIONS PROVIDERS (MOBILE AND INTERNET) OPERATING IN MOROCCO	114

12. ANNEXES	115
12.1 CIRCLES / NSO GROUP VPN SERVER CERTIFICATES	115
12.2 VERINT SALES PROPOSALS TO MOROCCO	117
12.3 ANNEX: PROFILES OF PEOPLE INTERVIEWED FOR THIS REPORT	118

DRAFT

GLOSSARY

TERM	DEFINITION
AUTHORITARIAN PRACTICES	A pattern of actions that entrench or concentrate power in ways that generally lead to or facilitate human rights violations. These can include surveillance, smear campaigns, and judicial harassment, used to silence dissent and shrink civic space.
CHILLING EFFECT	The fear produced by surveillance and repression that causes journalists, activists and human rights defenders to limit their speech, reporting or activism.
COMMAND AND CONTROL	The remote server infrastructure used by an attacker to communicate with, control and exfiltrate data from devices infected with spyware. Commonly abbreviated as 'C2'.
DEFAMATION MEDIA	Term used locally to describe media outlets aligned with state interests and used to carry out smear campaigns against dissidents, journalists and human rights defenders.
HIGHLY INVASIVE SPYWARE	<i>Highly invasive spyware</i> is spyware which can gain complete access to all data on a targeted device and whose functionality is not limited to accommodate the need for proportionality, or spyware whose use cannot be independently audited or verified in case of abuse.
HIRAK EL-RIF	The Hirak El-Rif movement was a series of demonstrations organized in the Rif region of northern Morocco in 2016 and 2017 demanding an end to the marginalization of their communities and making social justice related demands.
IMSI CATCHER	An <i>International Mobile Subscriber Identity catcher</i> is a device that imitates a mobile phone tower in order to identify nearby phones and intercept calls or data in real time.
JUDICIAL HARASSMENT	The use of legal proceedings, prosecutions or unfair trials to intimidate, silence or punish critics, journalists and human rights defenders.
MAKHZEN	A term used to refer to the governing apparatus of Morocco, centred on the monarchy and associated security and political elites.
MAN-IN-THE-MIDDLE (MITM)	A <i>man-in-the-middle</i> is an attacker who can read, modify, and block the network traffic from a target. A MITM capability can be used to censor the target or perform network injection attacks.
MASS SURVEILLANCE	The large scale interception, monitoring or collection of communications and data across networks or populations rather than against a single target.

TERM	DEFINITION
MOBILE FORENSICS TECHNOLOGIES	Mobile forensic tools or mobile data extraction products are specialized systems used by law enforcement or intelligence services to recover, analyse, and interpret data from mobile devices for legal or investigative purposes. Their tools can be used non-consensually to unlock devices or bypass device security mechanisms.
NETWORK INJECTION	<i>Network injection</i> is a technique where internet data packets are injected in the internet traffic of a target to block, intercept or manipulate their traffic.
OSINT	Open-source intelligence.
PHYSICAL INFECTION	The covert installation of spyware through temporary physical access to a target device.
PRE-INFECTED PHONES	Phones covertly loaded with spyware before being sold or otherwise passed to a target.
SMEAR CAMPAIGN	In this report, the term ‘smear campaign’ is used as a shorthand to refer to defamation and other forms of stigmatizing and harmful media and online harassment campaigns which serve to discredit, undermine or sully the reputation of the target.
SPYWARE	<i>Spyware</i> is software which enables an operator to gain covert access to information from a target computer system or device.
SS7	<i>Signaling System Number 7</i> is a set of signalling protocols and standards used in telephone networks to perform actions such as call-establishment, routing, and roaming between national and international mobile phone providers. The protocol was designed without modern security defences and has been exploited by commercial surveillance vendors to enable various attacks including location tracking and communications interception.
SURVEILLANCE-FOR-HIRE	The commercial market in which private companies provide governments with surveillance products or related services.
SYSTEM INTEGRATOR	A broker or intermediary that sources, combines, deploys and sometimes supports surveillance technologies from multiple vendors for a client.
TECHNO-AUTHORITARIANISM	A pattern of actions where governments, corporate actors and/or other powerful non-state actors use digital technologies to monitor, control and suppress populations to unduly build, retain or concentrate power.
TRANSNATIONAL REPRESSION	Surveillance, intimidation or harassment that extends beyond Morocco’s borders to target critics living abroad.
VPN SERVER	A virtual private network server.
ZERO-CLICK ATTACK	A zero-click attack is a surveillance industry marketing term for any vector which can infect a device without requiring a user action, such as clicking on a link.
1-CLICK ATTACK	A 1-click attack requires action from the target to enable the infection of their device, typically by opening a malicious link. Various social engineering techniques are used to trick the target into opening the link, including spoofing legitimate websites or news articles. If clicked on, the attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device.

ACRONYMS

WORD	DESCRIPTION
AMDH	<i>Association Marocaine des Droits Humains</i> (Moroccan Association for Human Rights)
APK	<i>Android Package Kit</i> , the standard file format for installing software on Android devices
ANRT	<i>Agence Nationale de Réglementation des Télécommunications</i> (National Telecommunications Regulatory Authority)
CNDP	<i>Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel</i> (National Commission for the Supervision of the Protection of Personal Data)
CODESA	<i>Collectif des Défenseurs Sahraouis des Droits Humains au Sahara Occidental</i> (Collective of Sahrawi Human Rights Defenders)
DGSN	<i>Direction Générale de la Sûreté Nationale</i> (Directorate-General for National Security), Morocco's national police force, referenced in the report as part of the wider security apparatus.
DGST	<i>Direction Générale de la Surveillance du Territoire</i> (Directorate-General for Territorial Surveillance), Morocco's domestic intelligence service.
HRD	<i>Human rights defender</i> ; a person who works to protect or promote human rights and who is one of the report's central categories of surveillance target.
IMEI	<i>International Mobile Equipment Identity</i> . A unique identifier assigned to a mobile device

SUMMARY OF COMPANIES AND SURVEILLANCE TECHNOLOGIES

This report features a number of companies, many of which have undergone extensive renaming, changed their corporate structure or been acquired. This table summarizes the primary companies featured in the report, their surveillance products (in italics), and the naming conventions that Amnesty has used for readability purposes in this report. The list is a non-exhaustive summary of corporate changes (renaming, restructuring and acquisitions) but provides a reliable guide for the purposes of this report.

Company	
Product	
NSO Group, Q Cyber Technologies SARL, Circles	NSO Group is a company based in Israel that develops and sells <i>Pegasus</i> , a form of zero-click spyware.
<i>Pegasus</i>	Q Cyber Technologies SARL is a Luxembourg-based company affiliated with NSO Group. It is a corporate entity within the NSO Group structure referenced in relation to Pegasus customer deployments and internal customer identification.
	Circles is a Bulgaria-based affiliate of the NSO Group. It develops an SS7-based phone-tracking technology and technical infrastructure associated with surveillance operations.
Hacking Team, Memento Labs	Hacking Team was an Italian surveillance company that produced the <i>RCS (Remote Control System)</i> spyware, including physical infection vectors and multi-platform device infection capabilities.
<i>RCS</i>	In 2019, Hacking Team was acquired by InTheCyber group and renamed as Memento Labs .
Verint, Cognytec, ACE Labs	Verint is a US technology company that provides a variety of software services and products, including surveillance products.
<i>Reliant 12, End Point Interception, WebIntPro</i>	Verint produced the Reliant 12 , used for the collection and analysis of telecommunications data. Verint also offered a spyware product line termed End Point Interception (EPI) .

Company

Product

In 2021, the cyber intelligence division of Verint was spun out as a separate entity, **Cognyte**, which specialises in cyber intelligence products. Cognyte created the social media monitoring product **WebIntPro**. Cognyte included the offensive cyber company **ACE Labs**, which closed in 2022.

Nexa Technologies, Amesys, Trovicor Intelligence, Datafusion

Eagle, Cerebro

Nexa Technologies was part of the Nexa group of companies which were operated mainly from France. The group was created in 2012 to take over the surveillance business of the French company **Amesys**. Amesys was a telecom and defence company, which created a mass-monitoring system called **Eagle**, capable of performing mass surveillance of internet (IP) traffic at the scale of a whole country. Amesys ceased its activities in the cyber-surveillance business in 2012, after the transfer of its assets to Nexa Technologies, which renamed Eagle as **Cerebro**.

In 2020, the Nexa group decided to abandon Nexa Technologies as a brand and began to operate under the commercial name **Trovicor Intelligence**. In 2024, the Trovicor group of companies rebranded as **Datafusion**.

Gamma Group, FinFisher

FinSpy

Gamma Group is a British-German company that produces surveillance products. FinFisher Labs is based in Germany. The companies developed the **FinSpy** spyware, which researchers identified as operating in Morocco.

Cellebrite

Cellebrite UFED

Cellebrite is a digital forensics and intelligence company headquartered in Israel.

Cellebrite produce the UFED (universal forensics extraction device) mobile forensic tool that is used to recover, analyse, and interpret data from mobile and other digital devices.

Interionet

Nighthawk

Interionet is an Israeli cyber intelligence company.

Interionet produce *Nighthawk*, a product that allows for remote intrusion into cameras.

Al Fahad Smart Systems, FSSysTech, Al Fahad Group, ETIMAD/EDGE

Al Fahad Smart Systems, also known as **FSSys Tech**, is a UAE-based surveillance broker. It is part of **Al Fahad Group** and is now part of **ETIMAD/EDGE**.

Maroc Telecom

Maroc Telecom is a former state company that is now majority owned by **E&** of the United Arab Emirates (UAE), although the Moroccan state maintains a 30% stake.

1. EXECUTIVE SUMMARY

“There are written laws, but they don’t apply. There are laws that no one respects. They don’t care about judicial authorization, warrants. Sometimes you can even a posteriori draw up the documents, do things in reverse. There’s complete impunity. We start with the verdict.”

Safir, former member of Direction Générale de la Surveillance du Territoire (DGST)

“A test”, “a guinea pig”: this is how agents of Morocco’s domestic intelligence services, the *Direction Générale de la Surveillance du Territoire* (DGST) described the human rights defender and academic Maâti Monjib when they chose him to be one of the first people targeted with NSO Group’s Pegasus spyware in 2017. But for Maâti Monjib, the outcome was anything but theoretical. His targeting by the DGST confirmed what he had long suspected – that he was under surveillance by the Moroccan authorities for his human rights work and his academic writing. It also laid bare his entire digital life to the authorities: his messages, calls, camera, location, contacts, and more. At the same time, Maâti Monjib was facing criminal prosecution and repression for his work. In 2015, he was subjected to a criminal trial on charges of receiving foreign funds to train journalists and was barred from leaving Morocco. Years later, he was sentenced to one year of imprisonment. In 2020, he was again subjected to trumped up criminal charges related to money laundering and embezzlement and Amnesty International called for his immediate and unconditional release. Throughout this period, he faced relentless smear campaigns from state-aligned news outlets and online actors. Although eventually pardoned in 2024, the harassment did not stop. As recently as 2025, videos of him circulated online claiming he was drinking alcohol, smoking shisha and “cavorting with his mistresses”. Maâti Monjib believes the strategy was not only to silence him, but to frighten others into silence. As he put it, paraphrasing a Moroccan proverb: “hit the big ones, and the little ones will be afraid”.

Maâti Monjib’s experience is far from unique. Simply for exercising their rights, Moroccan human rights defenders are routinely the victims of a combination of unlawful surveillance, smear campaigns, and judicial harassment or criminal prosecution. Agents of the DGST operate without judicial oversight or accountability and target in secrecy and with impunity those who dissent. The range of tools they deploy is broad, but the goal is clear: to blackmail, discredit, shame and, if necessary, imprison those who speak out in defence of human rights in Morocco.

This report provides the most detailed and comprehensive picture to date of the surveillance ecosystem that enables the Moroccan authorities to use repressive tactics to harass, discredit and ultimately silence human rights defenders. It draws on new testimony from sources who have worked inside the Moroccan intelligence services who were involved in the unlawful surveillance of human rights defenders; leaked surveillance data and targeting records internal to the government; leaked material from surveillance vendors; and original journalistic investigations carried out by Amnesty International’s research partners.

Morocco was among the first countries where activists and journalists were found to be targeted with advanced spyware tools, with evidence of Hacking Team spyware attacks revealed in 2012. Moroccan civil

society was again identified among the global set of Pegasus spyware targets in 2019, and the extensive scope of Morocco's surveillance against human rights defenders was brought to light during the 2021 Pegasus Project. This documented history of spyware and surveillance abuses makes Morocco a unique case in which to analyse how states exploit a range of surveillance technologies to target critics and limit the work of civil society.

Morocco's surveillance ecosystem relies on high-tech tools, including highly invasive spyware such as Pegasus, as well as old-fashioned techniques including following a target in person, taping conversations and everything in between. Personal devices are compromised. People are secretly videoed and audio recorded in detention, in their own offices and cars, and even in their own bedrooms. Phone calls are systematically recorded and spied upon. Location data is tracked, revealing daily movements, contacts and more. Phone shops sell mobile phones pre-infected with malware by DGST agents. Neighbours are recruited as informants to report on human rights defenders' (HRDs) daily movements and activities. All of these tactics extend not only to the targeted human rights defenders but also to their families, friends and professional networks, both inside Morocco and abroad. In short, for human rights defenders in Morocco, there is nowhere to hide and no way to escape the state's all-encompassing web of surveillance.

As a result, the most intimate details of human rights defenders' lives are an open book to the authorities – and are exploited to silence them. Data, including video and audio recordings of a personal, intimate or sexual nature, may be captured and at times shared with state-aligned media outlets, who conduct public smear campaigns aimed at sully the reputations of activists and discrediting them in the eyes of the Moroccan public. Women human rights defenders in particular, or women linked with prominent male targets, are subject to attempts to publicly shame them for real or perceived transgressions of conservative social norms. These campaigns can last for years and are promoted online by an army of state-affiliated commenters to boost the reach and visibility of the content. These campaigns are so well-known that the outlets through which they are most commonly conducted are referred to locally as the “defamation media”.

Together with unlawful surveillance and smear campaigns, human rights defenders have been repeatedly targeted with judicial harassment and politically motivated and/or trumped-up criminal charges, arrest, detention and imprisonment following unfair trials and on the basis of a legal framework which violates international standards. Some have been prosecuted for acts protected by their right to freedom of expression or association on charges which are not recognizable crimes under international law, such as broadly defined speech offences used to prosecute people for dissent or other legitimate expression. In some cases, HRDs are pressured to provide false testimony against others.

The targeting of human rights defenders is not limited to Morocco's borders. Those in exile, or who report from abroad, continue to be targeted for surveillance and smear campaigns. Even foreign officials and diplomats have been drawn in.

The wider result of these combined tactics is the creation of a profound chilling effect on other human rights defenders, and on any other potential dissent within society at large. With no way to know when they are being observed and recorded, facing unknown risks for family and friends, fearing public shaming or even imprisonment if they speak out, the cost of dissent in Morocco grows ever higher.

And yet, many continue to speak out and attempt to hold those in power to account. Their cases are highlighted in this report. Their stories underscore the urgent need for Morocco to end the impunity enjoyed by the DGST, reform its laws and practices, and respect, protect and fulfill the human rights of journalists and human rights defenders.

THE USE OF UNLAWFUL SURVEILLANCE IN MOROCCO

Covert surveillance does not in and by itself constitute a human rights violation. It can be conducted lawfully provided a number of guarantees are met, set out in the International Covenant on Civil and Political Rights (ICCPR), to which Morocco is a party, and related to the protection of the rights to privacy, opinion and expression. The Human Rights Committee determined that the right to privacy required that robust, independent oversight systems were in place regarding surveillance, interception and hacking. The UN General Assembly, in its resolution 73/179, noted that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.

Surveillance is unlawful even when undertaken in accordance with domestic legal procedures if these procedures violate or contravene international human rights standards. Surveillance is unlawful, for example, when conducted without judicial authorization and oversight as required under procedures governing its use.

Under international human rights law, Morocco must not only refrain from committing human rights violations, but must also protect people from abuses by private actors. Further, Morocco must not only

ensure the legality of surveillance conducted within its borders, but also extra-territorially. The use of spyware and other surveillance tools as mechanisms of transnational repression has been increasingly noted as a subject of concern by a growing list of UN authorities and experts.

In Morocco, surveillance is carried out by the DGST, often without legal authorisation, and for the unlawful purpose of targeting human rights defenders for their work. This surveillance extends not only to the human rights defenders themselves, but also to their families, legal representatives and social and professional networks. This surveillance is undertaken without independent oversight and is routinely carried out without regard for domestic legal procedures.

Under international law and standards, interference with the right to privacy is permissible only when it meets the requirements of legality, necessity, and proportionality, and is conducted for a legitimate purpose. Thus, surveillance undertaken to target human rights defenders because of their work in defence of human rights is unlawful under international human rights law and standards, regardless of whether it complies with the requirements of domestic legal procedure.

To meet their obligation to respect the right to privacy, it is crucial that the authorities have in place legal and other safeguards capable of preventing abuses of surveillance technology in practice. The lack of adequate judicial oversight, accountability measures or access to an effective remedy results not only in violations of the right to privacy of those targeted for surveillance, but also creates a chilling effect that causes journalists, activists, HRDs, and many other community members, to limit their speech, reporting or activism, thus reducing civic space for all.

While Morocco bears the primary responsibility for upholding human rights law, private companies, both domestic and international, also bear human rights responsibilities to avoid causing or contributing to human rights abuses. These obligations exist over and above domestic law.

The compatibility of surveillance measures with human rights law depends not only on the law and practice of state agencies, but also on the particular tools used. Mass surveillance, as carried out using tools like those purchased from Amesys or Verint, or via the extra-legal cooperation of telecommunications providers, is contrary to human rights law and standards. Many forms of modern highly invasive spyware used by the Moroccan authorities, such as NSO Group's Pegasus and Hacking Team's Remote Control System (RCS), are fundamentally incompatible with human rights due to their design. Amnesty International has called for a global ban on these forms of highly invasive spyware, because they allow unlimited access to devices and their use cannot be independently audited.

Additionally, privacy and other human rights can be violated through the use of a range of tools, even if they are not considered "surveillance" tools in the strict sense by their providers or users. This includes digital forensics tools, IMSI catchers, and so on. Nor does the lawfulness of surveillance depend on the technical sophistication of the devices used. Even the simple act of recording or listening in on a target must accord with international human rights law and standards.

INSIDE PEGASUS: HOW THE WORLD'S MOST NOTORIOUS SPYWARE HAS EVOLVED AND HOW IT WAS USED BY MOROCCO TO TARGET HUMAN RIGHTS DEFENDERS AND JOURNALISTS

For years, NSO Group's Pegasus spyware has been used to facilitate human rights violations around the world on a massive scale. As part of this report, Amnesty International drew on previously unpublished internal NSO Group marketing material and technical materials which were disclosed as part of a long-running US civil court case initiated by WhatsApp and Meta, and which provide the most complete picture to date of how the Pegasus system is built, operated and maintained.

This new analysis provides valuable findings on spyware accountability, including outlining the degree to which the system used by government clients requires ongoing maintenance and support by NSO Group to enable its ongoing functioning. The newly disclosed documents also independently corroborate the authenticity and accuracy of the leaked dataset foundational to the original *Pegasus Project* investigation.

This enhanced understanding of Pegasus has allowed Amnesty International to build upon its previous reporting regarding the use of NSO Group's Pegasus spyware in Morocco. This current report documents that, despite official denials, the Moroccan authorities used Pegasus spyware between 2017 and 2021, and possibly later. Amnesty International documents how the use of Pegasus in Morocco evolved in tandem with developments in the technology itself. Forensic evidence demonstrates how a variety of "vectors" (exploits and infection techniques) were used to attack human rights defenders' devices, including: "1-click attacks", which typically rely on the victim clicking on a malicious link; "zero-click attacks", which can surreptitiously infect a target without them having to click a link, or indeed take any action at all; and network injection attacks, which were dependent on using the Maroc Telecom network.

This report also draws on the aforementioned internal NSO Group documentation to demonstrate the steps NSO Group takes to register unique attack infrastructure for each customer. This finding validates the methodology of the spyware accountability community in linking clusters of spyware attacks to the same operator. This is of particular importance in the case of the Moroccan authorities' use of the tool, since it can be used to establish that the same customer is responsible not just for attacks on human rights defenders in Morocco, but also for unlawful surveillance attacks using Pegasus spyware against Moroccan activists and journalists living abroad, as well as certain activists, journalists, diplomats and other officials who are nationals of other countries.

HOW A SHADOWY NETWORK OF SURVEILLANCE COMPANIES FACILITATES A RANGE OF SURVEILLANCE TECHNIQUES IN MOROCCO

While the use of Pegasus spyware by the Moroccan authorities is of great significance given the capabilities and impacts of highly invasive spyware, it is only one digital tool among many in Morocco's repressive surveillance ecosystem. The Moroccan government relies on a range of techniques as well as tools purchased – without public scrutiny – from various corporate actors based in Israel, the EU and the United States of America. It also relies on the extra-judicial cooperation of at least one domestic telecommunications provider.

This report documents that in addition to contracts with NSO Group, two Moroccan security agencies, the DGST and the High Council for National Defence (*Conseil Supérieur de la Défense Nationale*, CSDN), had contracts with the now defunct Italian spyware company Hacking Team (later rebranded as Memento Labs) since at least 2009. Morocco was one of the top customers of the company's Remote Control System (RCS) spyware.

Research from other civil society organizations has also identified instances of FinSpy spyware, produced by the British-German network of companies Gamma Group and FinFisher, being used in Morocco.

In addition to targeted surveillance technologies, Morocco has used a number of mass surveillance technologies which allow for the widespread and bulk monitoring, interception, storage or analysis of user materials. For example, since December 2009, Morocco has used the Eagle system (later rebranded as Cerebro) from French telecom and defence company Amesys (later renamed Nexa Technologies, and subsequently Trovicor Intelligence, and which was renamed again as Datafusion in 2024). This technology is capable of monitoring internet (IP) traffic at a country-wide level. The project, code-named "Popcorn" by Amesys, involved the deployment of the Cerebro mass internet interception technology in Morocco.

The report also documents Morocco's 2014 purchase of the US company Verint's Reliant 12 system, which enables the unified collection and analysis of telephone communications, data from mobile internet service providers, and internet traffic data.

The DGST have used IMSI catchers, devices which are designed to replicate mobile phone antennas and can catch the data from nearby devices, including from encrypted messaging apps prior to transit, allowing agents to spy on activists' phones and to conduct surveillance of human rights defenders.

The DGST also have recourse to the Universal Forensic Extraction Device (UFED) from the Israeli company Cellebrite. This surveillance tool allows complete access to a device's data while it is in an operator's physical custody. The authorities have used situations such as detention or airport transits to unlawfully access the devices of human rights defenders without their knowledge.

Morocco is also a customer of cyber intelligence company Cognyte, which was spun off in 2021 from US-based company Verint Systems and whose tools allow customers to control fake social media accounts ("avatars") in order to gather intelligence about social media users or to launch social engineering attacks.

According to former DGST agent *Safir*, an essential element of the DGST's surveillance capabilities is the cooperation of a domestic telecommunications provider. He described how DGST agents have direct access to data and communications over the network, including accessing calls that agents can listen to or transcribe at will. The described surveillance capabilities are consistent with functionality offered by Verint's RELIANT product, a mass surveillance system which was sold to Moroccan authorities in the mid-2010's, according to internal Verint sales records. The sales records also list Maroc Telecom as the potential purchaser of Verint network interception products as part of the wider system. Forensic investigations have confirmed that Maroc Telecom's network has been used to facilitate spyware attacks through a technique known as 'network injection'.

Unregulated access to private telecommunications infrastructure and data has also enabled the DGST to conduct network injection attacks to install spyware and freely track location data. By providing identifying

technical information to DGST outside of legal processes, this provider also facilitates unlawful surveillance by DGST.

The DGST and other agencies also rely on less technologically sophisticated tools, such as hidden audio and video recording devices placed in homes, cars, offices, public spaces, and places of detention. GPS trackers can track a target's location over time, which DGST agents can view through their own bespoke interface. These techniques are used in combination with human recruits charged with reporting on the activities of human rights defenders in their orbit or with access, for instance cafe staff, local merchants or neighbours, targeted for unlawful surveillance.

DGST agents also carry out video surveillance via networks of public video cameras, and can access private cameras via a tool called NightHawk, a device the size of a small suitcase produced by Israeli cyber intelligence company InteriorNet.

To deploy this range of tools, the DGST relies on partner agencies and a host of techniques. For example, RCS spyware was deployed using physical infection of devices, often via USB drives, targeting people during, for example, airport transfers, or by physically infecting devices in internet cafes.

Spyware has also been deployed by being pre-installed onto mobile devices that are then placed in shops and sold to targets.

While there's no doubt that implementing strong digital security practices can make it more difficult for the DGST to surveil human rights defenders, with so many techniques in use this broader surveillance ecosystem can be almost impossible to escape.

THE USE OF SMEAR CAMPAIGNS TO DISCREDIT HUMAN RIGHTS DEFENDERS

This report documents that one of the key purposes of unlawful surveillance of human rights defenders is to discredit them publicly.

In several instances documented in this report, private information gathered through DGST surveillance operations against human rights defenders later appeared in media coverage and was used in coordinated smear campaigns against them. These campaigns were frequently carried out by media outlets politically aligned with the authorities, such as Chouf TV, Barlamane and Le360, and often featured private images and videos of targets. Smear campaigns of a sexual nature were used in attempts to discredit women human rights defenders or women linked with prominent journalists and human rights defenders in particular. While Amnesty International could not independently verify the source of the information disclosed by these media outlets, the nature of the material, including intimate images and private communications, and the apparent absence of any other plausible means through which these outlets could have obtained access to it, raise serious concerns that information obtained through surveillance may have been disclosed to, shared with, or otherwise made available to media actors by Moroccan authorities.

These campaigns are amplified online. Examples of coordinated inauthentic social media behaviour campaigns targeting human rights defenders in Morocco have twice been identified by Meta, Facebook's parent company. According to insider testimony, such campaigns are assisted by state-funded commentators whose role it is to comment on, and therefore raise the visibility of online smear campaigns.

These smear campaigns continued often after human rights defenders were imprisoned, released or pardoned, and even after they left Morocco.

Morocco is in violation of its obligation to respect the right to privacy of human rights defenders where it shares or leaks surveillance data to media outlets, or otherwise directly supports smear campaigns harassing human rights defenders. In addition, under international human rights law, the Moroccan authorities must also protect and fulfil the rights of human rights defenders by taking steps to protect them from smear campaigns by private actors, and they must also take steps to fulfil the rights of human rights defenders by creating a safe and enabling environment in which they can carry out their work.

JUDICIAL HARASSMENT AND REPRESSION

In conjunction with unlawful surveillance and defamatory smear campaigns, human rights defenders have been repeatedly targeted with criminal prosecution in the form of politically motivated and/or trumped-up charges, arrest, detention and imprisonment following unfair trials, and/or prosecuted for acts the punishment of which is contrary to international law.

Many such trials have been marred by violations of detainees' rights and basic fair trial rights. Often, human rights defenders have faced trumped-up charges or charges that criminalized their legitimate activities in violation of human rights law. Sahrawi activists and people active in the Hirak El-Rif protest movement were

particularly singled out for their protest activities and activism, which were criminalized as “threatening the internal security of the state”.

This report also documents cases in which human rights defenders were pressured by the authorities to provide false testimony against other human rights defenders.

While some of the human rights defenders targeted in this way have been released or pardoned, many remain in detention.

CONCLUSION

The Moroccan authorities’ combined use of unlawful surveillance, judicial harassment and repression has resulted in violations of numerous human rights, including the rights to privacy, liberty, and to freedom of expression, association and peaceful assembly.

It has also created profound chilling effects, causing psychological, social and professional harms to those targeted, and deterring others and society at large from the lawful exercise of human rights.

RECOMMENDATIONS:

TO THE MOROCCAN AUTHORITIES:

- Release people imprisoned in connection with the lawful exercise of their human rights.
- Immediately cease surveillance of human rights defenders and journalists lawfully exercising their human rights and respect and ensure their right to privacy.
- Undertake legislative reforms needed to implement a human rights regulatory framework governing surveillance that is capable of preventing abuses in practice, including by the DGST and other security agencies. Until such a framework is implemented, a moratorium on the purchase, sale, transfer and use of surveillance equipment should be enforced.
- Ensure an independent, effective and systemic investigation into the DGST, including all reported cases of unlawful surveillance, hold all those responsible to account and provide for effective remedies for victims, including meaningful pathways for judicial redress, for physical and mental harm, as well as loss of livelihood.
- Cease any and all participation by state actors in defamatory smear campaigns against human rights defenders and journalists, including on social media, and take steps to protect human rights defenders from such campaigns in media outlets.

TO ALL STATES:

- Deny export authorization of spyware, digital forensics tools, and other privacy-invasive technology to Morocco until such time as there has been a thorough, independent and effective investigation into unlawful surveillance of journalists, political activists and human rights defenders, and a system of human rights safeguards is in place capable of preventing human rights abuses in practice.
- Prohibit companies from producing, selling, transferring or supporting highly invasive spyware, the functionality of which cannot be limited and whose use cannot be independently audited.

TO STATES FROM WHICH SURVEILLANCE OR OTHER PRIVACY-INVADING TECHNOLOGY IS EXPORTED, SOLD OR BROKERED:

- Conduct an investigation into the export, sale, transfer or brokering of technology linked to human rights abuses in this report, and revoke export licences where there is evidence or significant risk of its link to human rights abuses.
- Prevent companies from brokering or otherwise facilitating the sale, transfer or support of surveillance and other privacy-invading technology to Morocco until such time as there has been a thorough, independent and effective investigation into unlawful surveillance of journalists, political activists and human rights defenders, and a system of human rights safeguards is in place capable of preventing human rights abuses in practice.

TO COMPANIES INVOLVED IN SUPPLYING SURVEILLANCE AND OTHER PRIVACY-INVADING TECHNOLOGY TO MOROCCO:

- Halt all sales, exports and transfers of all surveillance technologies to Morocco, as well as all brokering or other support for such sales, transfers or support, until such time as there has been a thorough, independent and effective investigation into unlawful surveillance of journalists, political

activists and human rights defenders, and a system of human rights safeguards is in place capable of preventing human rights abuses in practice.

- Implement robust mechanisms for reparations, including compensation for targets of unlawful surveillance or other forms of redress.

TO TELECOMMUNICATIONS PROVIDERS (MOBILE OR INTERNET) IN MOROCCO:

- Carry out adequate human rights due diligence in order to identify, prevent, mitigate and account for adverse human rights impacts, including in relation to surveillance, in particular by thoroughly assessing the risks of unlawful data sharing, and making risk assessments public.
- Develop accessible and safe grievance mechanisms through which complaints regarding surveillance technology and its use can be addressed effectively. These mechanisms should be available in all countries and measures must be taken to ensure these mechanisms are accessible to all.

2. METHODOLOGY

This report builds on an extensive body of first-hand documentation, technical investigations and source interviews conducted by Amnesty International between mid-2019 and May 2026 on the unlawful surveillance practices of the Moroccan authorities.

Most significantly, this report draws on new and unpublished testimony from sources who worked within the Moroccan intelligence services; leaked surveillance data and internal targeting records; leaked material from surveillance vendors; and original journalistic investigations conducted by research partners.

This report focuses on unlawful surveillance in Morocco, documenting both the targeting of journalists and human rights defenders (HRDs) in the course of their legitimate activities, and how safeguards against abuses are either absent or evaded. Furthermore, the report provides evidence of the use of tools, such as highly invasive spyware, which are unlawful by design, given the level of interference with the right to privacy. While states can conduct surveillance in line with international human rights law, such surveillance is unlawful if people are targeted for the legitimate exercise of their rights, or in a discriminatory fashion because of their identity. In cases where there may be a legitimate basis to conduct surveillance, for example, where there are reasonable grounds to suspect criminal wrongdoing, such surveillance may still be unlawful if there are inadequate safeguards against abuse.¹

Amnesty International conducted extensive interviews with a whistleblower who was a former member of Morocco's domestic intelligence services, the *Direction Générale de la Surveillance du Territoire* (DGST), who directly participated in numerous surveillance operations during their decade-long employment at the DGST. To ensure their safety and to avoid retribution, Amnesty International and media partners in 'The Pegasus Project: Inside Morocco's Surveillance Machine'² have used the pseudonym *Safir* for this whistleblower. Amnesty International has verified *Safir's* identity, employment history and many key aspects of their testimony via independent sources. Further verification was undertaken by Forbidden Stories and media partners of the *Pegasus Project: Inside Morocco's Spying Machine* (see below in this section). Oral interviews with *Safir* conducted by the Moroccan journalist Hicham Mansouri have also been cited in this report.

Safir's testimony was further verified and cross-checked against independent technical evidence and the testimony of other sources, including two Moroccan ex-intelligence officials and surveillance industry professionals with knowledge of Morocco's surveillance practices. Many of the key claims made by *Safir* are supported by leaked data and other unpublished material reviewed during the investigation, including technical records, the testimony of surveillance targets, and further research into the activities of Morocco's intelligence services. This whistleblower testimony provides a critical and unique opportunity to peel back the many layers of secrecy, fear and uncertainty which surround Morocco's extensive use of surveillance technologies against civil society. This testimony and the leaked materials also provide a rare holistic view into how a national surveillance apparatus can combine cutting-edge digital surveillance with more traditional surveillance methods to target human rights defenders.

The leaked surveillance data – reviewed and analysed by Amnesty International – identifies specific individuals selected for surveillance using multiple different systems, including NSO Group's Pegasus spyware, Hacking Team's RCS spyware, and phone geolocation systems. A subset of this leaked material also included raw surveillance data, such as photos and audio recordings covertly gathered from phones

¹ UN Office of the High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age* (UN Doc. A/HRC/27/37), 30 June 2014, <https://docs.un.org/en/a/HRC/27/37>, para. 21.

² Forbidden Stories, *Pegasus Project: Inside Morocco's spying machine*, 16 July 2026, forbiddenstories.org/projects_posts/pegasus-project-inside-moroccos-spying-machine/

infected with spyware by Moroccan authorities. Additionally, Amnesty International analysed two distinct Android spyware agents which were used in recent years to target activists and journalists in Morocco and abroad (see Section 5.3).

This report is published as part of the *Pegasus Project: Inside Morocco's Spying Machine*, a research collaboration of 14 media partners coordinated by the investigative journalism network Forbidden Stories.³ Amnesty International worked with the Forbidden Stories consortium to analyse and verify an unprecedented range of materials on surveillance technologies and operations. Media partners in the *Pegasus Project* have verified key findings with sources in the cyber-surveillance industry, European intelligence and policing organizations, and with Moroccan sources knowledgeable about the inner workings of the security services, including the two ex-intelligence officers mentioned above. Members of the Forbidden Stories consortium collaborated on research leads, shared interview transcripts, and conducted fact checking on the overall project findings. Each partner remains solely responsible for the content of their own publications; however, the source material is common to all media partners. Where Amnesty International drew on interviews or analysis of consortium partners, this is referenced in the report.

In addition, Amnesty International conducted in-person and remote interviews with 10 journalists and human rights defenders from Morocco who have endured repression in the form of surveillance, defamation and/or judicial harassment. Of these, four currently reside in Morocco. Informed consent was obtained to conduct all interviews and to publish their testimony in this report. Interviews with individuals located in Morocco were conducted remotely. Amnesty International provided no remuneration to the interviewees or sources in exchange for testimonies. The interviewees who consented to be named in this report are, in alphabetical order: Fouad Abdelmoumni, Afaf Bernani, Mohamed Majaoui, El Mahjoub Maliha, Hicham Mansouri, Maâti Monjib, Kholoud Mokhtari, Omar Radi, Soulaïman Raïssouni and Ali Salem Tamek.

Other sources used by Amnesty International in conducting research for this report include satellite imagery analysis, image geolocation, company records, trade data and other material on the workings of the cyber-surveillance industry, as well as extensive media reports, UN agency reports and reports from human rights organizations. Additionally, the research team carried out analysis of content from online news outlets and social media platforms, specifically focusing on disinformation and defamatory material targeting Moroccan civil society.

As part of the research conducted for this report, Amnesty International, in coordination with Forbidden Stories, reanalysed the leaked dataset of Pegasus targeting information, which was foundational to the 2021 Pegasus Project publication.⁴ Amnesty International found that almost 13,000 unique phone numbers were selected as potential targets by the Moroccan Pegasus customer, the DGST; the DGST was the largest customer in the dataset based on unique targets. Since the earlier publication of the original *Pegasus Project* reporting, the full original dataset of around 50,000 numbers – which included numbers targeted by a dozen other Pegasus customers – was further validated by authorities in Poland, France, and Hungary, who confirmed that individuals whose phone numbers were identified in the list were in fact targeted and infected by Pegasus. Further forensic investigations were carried out to confirm spyware infections consistent with the dataset.

Safir named specific individuals holding key senior positions within the DGST, including the officers responsible for overseeing these spyware surveillance operations and telecommunication interception. *Safir* also provided work phone numbers for some DGST staff members who they alleged were involved in testing and deploying NSO Group's Pegasus spyware in Morocco.

The analysis in Chapters 4-6 of this report, addressing the technical capabilities and surveillance technologies used by the DGST, is based on technical material, leaked documentation, *Pegasus Project* data and other material that is consistent with, but independent of, *Safir's* testimony. Chapter 7 draws more heavily on whistleblower evidence to map how the various surveillance technologies (analysed in Chapter 5) and disparate tactics are woven together to build a multi-layered net of surveillance.

ACKNOWLEDGEMENTS

Amnesty International would like to express our deepest gratitude to *Safir* and the human rights defenders who bravely shared their testimonies with us.

While the *Pegasus Project: Inside Morocco's Spying Machine* has been a collaboration between multiple media partners, it is built on an initial body of research by the Moroccan journalist and human rights

³ Forbidden Stories, *Pegasus Project: Inside Morocco's spying machine*, https://forbiddenstories.org/projects_posts/pegasus-project-inside-moroccos-spying-machine/ (accessed on 4 August 2026).

⁴ Amnesty International Security Lab, Case study: The Pegasus Project, <https://securitylab.amnesty.org/case-study-the-pegasus-project/> (accessed on 4 August 2026).

defender Hicham Mansouri. Since 2023, Hicham Mansouri has conducted hundreds of hours of interviews with *Safir*, human rights defenders and other sources. Transcripts of some of these interviews were shared with Amnesty International, and Hicham Mansouri also conducted fact checking for this report. We extend to him our sincerest thanks and appreciation. Hicham Mansouri is publishing his research on this project with the Moroccan media outlet Hawamich.⁵

DRAFT

⁵ Hawamich Media, *البيات المراقبة عن بعد.. تحقيق من داخل منظومة التجسس المغربية* [Remote monitoring mechanisms. An investigation from within the Moroccan spy system], 17 July 2026 <https://hawamich.info/11983/> (in Arabic).

3. BACKGROUND

Journalists, human rights defenders and whistleblowers play a key role in exposing authoritarian practices carried out by states.⁶ Reducing or limiting criticism levelled at those in authority is a key strategy used by states to evade accountability and prevent discussions on a government's human rights record in order to shrink civic space and build, accumulate or consolidate unfettered power. A core objective of these tactics is to spread fear and send a chilling message to limit further potential dissent. As a result, individuals engaged in the defence of human rights or otherwise critical of the government are often among the first to be targeted and silenced by the authorities. So too in Morocco. For decades, Amnesty International and other human rights organizations⁷ have documented repression of journalists and human rights defenders across the country.

Journalists and civil society in Morocco operate in a highly restricted environment and face a variety of authoritarian practices, including unlawful surveillance, smear campaigns and judicial harassment. This is the three-pronged strategy facing human rights defenders that works to silence dissent, attack media freedom, shrink civic space and entrench power.⁸

Physical surveillance targeting civil society is a long-standing tactic used by the Moroccan authorities.⁹ It was particularly prevalent during the period from the mid-1960s to the mid-1990s, known as the 'Years of Lead'. Interviewees for this report told Amnesty International that they had been subjected to physical surveillance: they reported the presence of cars in front of their houses and strangers following activists on foot. As technology and the surveillance industry have evolved over the years, so too have methods of surveillance. Physical surveillance tactics are still used today but are accompanied and reinforced by planted surveillance tools such as cameras, microphones and location (GPS) trackers. Digital surveillance is one of the pillars of techno-authoritarianism¹⁰, a pattern of actions where governments, corporate actors and/or other powerful non-state actors use digital technologies to monitor, control and suppress populations to unduly build, retain or concentrate power.

Despite a royal pardon from King Mohammed VI in July 2024 for around 2,460 prisoners,¹¹ Moroccan authorities continue to repress dissent and target journalists, activists and government critics using surveillance, along with other tactics in their repression toolbox. Several of the human rights defenders interviewed for this research described being subjected to surveillance as a "way of life" in Moroccan civil society. Consequently, individuals take precautions to varying degrees, depending on their previous experience of being surveilled. All interviewees indicated that they were aware of the capacity of the

⁶ International human rights law and standards do not define authoritarian practices. Political theorist Marlies Glasius defines authoritarian practices as "patterns of action that sabotage accountability to people over whom a political actor exerts control, or their representatives, by means of secrecy, disinformation and disabling voice". For more information, see Marlies Glasius, "What authoritarianism is... and is not: A practice perspective", May 2018, International Affairs, Volume 94, Issue 3, <https://doi.org/10.1093/ia/iiv060>; and Marlies Glasius, *Authoritarian Practices in a Global Age*, 2023.

⁷ For example, Moroccan Association for Human Rights (*Association Marocaine des Droits Humains*, AMDH): <https://amdh.org.ma/> (in Arabic).

⁸ In a 2022 report, Human Rights Watch described these approaches as Morocco's "playbook to crush dissent". See Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent, 2022, <https://www.hrw.org/report/2022/07/28/theyll-get-you-no-matter-what/moroccos-playbook-crush-dissent>

⁹ Ahmed Boukhari, *Le secret: Ben Barka et le Maroc – Un Ancien Agent des Services Spéciaux Parle [The Secret: Ben Barka and Morocco – A Former Special Services Agent Speaks Out]*, 2022 (in French).

¹⁰ Florence G'sell, "Digital Authoritarianism: From state control to algorithmic despotism", 30 January 2025, available at SSRN, papers.ssrn.com/sol3/papers.cfm?abstract_id=5117399

¹¹ Amnesty International, *The State of the World's Human Rights: April 2025* (Index: POL 10/8515/2025), 28 April 2025, <https://www.amnesty.org/en/documents/pol10/8515/2025/en/>, p. 263.

Moroccan authorities to intercept communications, with most using end-to-end encryption wherever possible in their confidential exchanges.

The information gathered by authorities from their surveillance operations can be used to fuel defamation or smear campaigns against dissidents, or be submitted as “evidence” to justify their arrest or against them in unfair trials. This is not always done covertly. In fact, these tactics are often used so brazenly that human rights defenders, journalists and government critics routinely self-censor to protect themselves.

3.1 PROSECUTIONS AND HEAVY PRISON SENTENCES FOR EXPRESSION

Targeted muzzling of online and offline expression is one of the strategies used by the Moroccan authorities to crack down on dissent. Moroccan authorities continue to investigate, prosecute and imprison journalists and activists for speaking critically about the government and particularly the King, as well as Western Sahara and religion. The Moroccan Penal Code includes a range of speech offences that are broadly defined, not recognizable offences under international law, and that provide heavy prison sentences for acts protected by the right to freedom of expression.

For example, in July 2025, human rights defender Saida El-Alami was detained on charges linked to her online activism. In September, a court sentenced her to three years in prison on charges of “spreading false information”, “insulting a public institution”, and “insulting a legally organized body”, all crimes under Moroccan law.¹² Saida El-Alami, a member of the collective “Moroccan Women against Political Detention”, had previously been imprisoned in 2022 on separate charges regarding social media posts in which she publicly denounced the harassment she faced at the hands of the police and criticized the authorities’ repression of journalists and activists.¹³

Those targeted by the criminalization of critical speech are often human rights defenders or activists. In 2023, the Rabat Court of Appeal sentenced journalist and member of the Moroccan Association for Human Rights (AMDH), Rida Benotmane, to 18 months in prison on charges relating to social media posts and YouTube videos dating from 2021 in which he criticized abuses by the security forces, called for the release of political detainees and accused the government of oppressing free speech.¹⁴ Benotmane was released in March 2024, after serving his full sentence.¹⁵

Mohamed Ziane, an 83-year-old human rights lawyer and ex-minister for human rights, knows better than most about the arsenal of oppressive tactics deployed by the Moroccan authorities against critical voices. Ziane resigned from his role in the Moroccan government in 1996, and since 2011 has been an outspoken critic of the authorities and the King and publicly defended a number of activists and journalists, including Nasser Zefzafi, a key figure in the Hirak El-Rif movement. The Moroccan authorities had already arrested and sentenced Ziane to three years’ imprisonment in 2022, on bogus charges, including defamation and marital infidelity, after he criticized the director of the Moroccan national security forces in reaction to a defamatory video.¹⁶ In 2025, additional charges were brought against him following statements he made from prison criticizing the King.¹⁷ This led to a sentence of a further three years, which the Court of Appeal refused to merge with his previous sentence.¹⁸

Even online commentary related to the authorities’ response to the 2023 El Haouz earthquake can result in a prison sentence. For example, in January 2025, Said Ait Mahdi, an activist who criticized the kingdom’s response to the earthquake, was sentenced to three months’ imprisonment for “defamation” and “insulting

¹² Amnesty International, *The State of the World’s Human Rights: April 2025* (previously cited).

¹³ Amnesty International, “Morocco: Stop criminal investigations against human rights defenders over social media posts”, 7 April 2022, <https://www.amnesty.org/en/latest/news/2022/04/morocco-stop-investigation-human-rights-defenders/>

¹⁴ Amnesty International, “Morocco/Western Sahara: Further information: Human rights defender’s conviction upheld: Rida Benotmane” (Index: MDE 29/6493/2023), 28 February 2023, <https://www.amnesty.org/en/documents/mde29/6493/2023/en/>

¹⁵ Frontline Defenders, “Rida Benotmane released after serving a sentence of 18 months in prison”, 29 March 2024, <https://www.frontlinedefenders.org/en/case/rida-benotmane-released-after-serving-sentence-18-months-prison>

¹⁶ Amnesty International, “Morocco: Human rights lawyer sentenced in absentia: Mohamed Ziane” (Index: MDE 29/6397/2023) <https://www.amnesty.org/en/documents/mde29/6397/2023/en/>; Bladi.net, “Morocco bars ex-minister from travel after criticizing king’s absence”, 15 November 2022, <https://en.bladi.net/morocco-bars-minister-from-travel-criticizing-king-absence,97802.html>

¹⁷ The Times, “Morocco jails ex-minister for criticising ‘absent’ king”, 22 July 2024, <https://www.thetimes.com/world/africa/article/morocco-jails-former-minister-for-criticising-king-vcs16k0pg>

¹⁸ ACCORD, “Morocco: COI Compilation - December 2025 (Reporting period: January 2023 to August 2025)”, https://www.ecoi.net/en/file/local/2135028/ACCORD_Morocco_December_2025.pdf; Yabiladi, “Rabat court rejects Mohamed Ziane release request”, 4 June 2026, <https://en.yabiladi.com/articles/details/195961/rabat-court-rejects-mohamed-ziane>

public officials” after he called for more aid to the affected populations and faster reconstruction. In March 2025, the Rabat Court of Appeal, in Morocco’s capital, added one year to his sentence.

Moroccan authorities continue to be particularly intolerant of all expression and assembly related to the rights of Sahrawis in Western Sahara.¹⁹ The Collective of Sahrawi Human Rights Defenders (CODESA) regularly reports on arbitrary arrests of Sahrawi activists, prolonged surveillance, house arrests of entire families and systematic censorship tactics used against protest organizers. In Laayoune and other cities in Western Sahara, Moroccan security forces regularly disperse peaceful demonstrations that call for Sahrawi independence and self-determination, leading to arrest and prosecution of Sahrawi activists.

Almost all of the human rights defenders interviewed for this research continue to be subjected to harassment by government-aligned news websites and other media outlets. This phenomenon plays a central role in manipulating public opinion and threatening the safety of those targeted by these campaigns.²⁰

Unlawful surveillance and judicial harassment of activists are accompanied by public smear campaigns aimed at undermining their public reputation. These campaigns, which take place online and over traditional media, are so commonplace that outlets known to conduct them are colloquially referred to as the “defamation media”.

On 24 December 2025, Morocco’s Parliament adopted Draft Law No. 26.25, which restructured the National Press Council (*Conseil National de la Presse*), effectively increasing government control over the media. Human rights groups expressed concern that this could potentially result in a renewed chilling effect on media freedom in Morocco.²¹ In February 2026, Morocco’s Constitutional Court declared several provisions of the draft law unconstitutional and ruled that amendments were necessary. The government submitted an amended version, Draft Law No. 09.26, which the Moroccan parliament approved in June 2026.²²

The use of repressive laws that criminalize legitimate forms of dissent by human rights defenders, journalists and activists is a key component of authoritarian practices that Morocco has used to sabotage accountability and entrench power, including by instilling a climate of fear and self-censorship.²³

Amnesty International and other civil society organizations have documented various cases of judicial harassment of Moroccan human rights defenders and journalists in recent years.²⁴ For this research, Amnesty International spoke with the following individuals who have each experienced judicial harassment of some kind: Fouad Abdelmoumni, Afaf Bernani, Mohamed Majaoui, Hicham Mansouri, Maâti Monjib, Omar Radi, Soulaïman Raïssouni and Ali Salem Tamek. Judicial harassment for these individuals has taken various forms, including denial of fair trial procedures and politically motivated convictions for financial irregularities, espionage and defamation.²⁵

The long reach of the Moroccan authorities’ surveillance and harassment practices also extends to people living outside of Morocco. Amnesty International and others²⁶ have documented cases of transnational repression, whereby Moroccan and Sahrawi human rights defenders and journalists living in other countries are harassed digitally or in person. This harassment is conducted through digital surveillance, smear campaigns, criminalization, and sometimes physical surveillance. As Fouad Abdelmoumni, who now lives in

¹⁹ Amnesty International, “Morocco/Western Sahara: Targeted Crackdown of Sahrawi Activists” (Index: MDE 29/4404/2021), 19 July 2021, <https://www.amnesty.org/en/documents/mde29/4404/2021/en/>

²⁰ Le Desk, “110 journalistes marocains dénoncent la prolifération de médias de diffamation”, 16 July 2020, [ledesk.ma/2020/07/16/110-journalistes-marocains-denoncent-la-proliferation-de-medias-de-diffamation/](https://www.ledesk.ma/2020/07/16/110-journalistes-marocains-denoncent-la-proliferation-de-medias-de-diffamation/)

²¹ Article 19, “Morocco: Establish truly independent Press Council following ruling”, 09 March 2026, <https://www.article19.org/resources/morocco-establish-truly-independent-press-council-following-ruling/>; Article 19, <https://www.article19.org/resources/morocco-establish-truly-independent-press-council-following-ruling/>

²² Article 19, “Morocco: Media sector left out of consultations for new press council law”, 6 July 2026 <https://www.article19.org/resources/morocco-media-sector-left-out-of-consultations-for-new-press-council-law/>

²³ Amnesty International and others, *Dissent on Trial: Strategies to Counter Rising Criminalization* (Index: POL 40/0502/2025), 25 November 2025, <https://www.amnesty.org/en/documents/pol40/0502/2025/en/>

²⁴ See, for example, Amnesty International, “Morocco/Western Sahara: Stop the judicial harassment of Sahrawi human rights defenders” (Index: MDE 29/003/2007), 5 February 2007, <https://www.amnesty.org/en/documents/mde29/003/2007/en/>; Amnesty International, “Morocco: Release human rights defender prosecuted on trumped up charges”, 27 January 2021, <https://www.amnesty.org/en/latest/press-release/2021/01/morocco-release-human-rights-defender-prosecuted-on-trumped-up-charges/>; Amnesty International, “Morocco: Journalist targeted by authorities faces trial”, 6 April 2021, <https://www.amnesty.org/en/latest/press-release/2021/04/morocco-journalist-targeted-by-authorities-faces-trial/>

²⁵ See Human Rights Watch, “*They’ll Get You No Matter What*” (previously cited).

²⁶ See for example: The Citizen Lab, No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression, December 2024, <https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>; and European Parliament, REPORT of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html (para 361).

Europe, told Amnesty International: “From what I read in the [defamation] press, it’s clear they’re on top of what I’m doing and where I’m going. The transformation of the world with digital tools has rendered borders secondary.”²⁷

DRAFT

²⁷ Interview by phone with Fouad Abdelmoumni, February 2026.

4. INSIDE PEGASUS: THE EVOLUTION OF THE WORLD'S MOST NOTORIOUS SPYWARE SYSTEM

NSO Group's Pegasus spyware has been used to facilitate human rights violations around the world on a massive scale. Amnesty International calls for a global ban on Pegasus and other forms of highly invasive spyware, because they allow unlimited access to a device and their use cannot be independently audited, and therefore incompatible with international human rights law. This chapter builds on previous technical reports and forensic investigations by Amnesty International's Security Lab in order to present the most complete analysis to date of Pegasus spyware and how it is used by NSO Group customers.²⁸ It provides important background context for chapter 5, which documents the use of Pegasus spyware by Morocco.

The chapter draws heavily on confidential customer documentation and internal NSO Group records which were disclosed as part of a long-running civil case taken by WhatsApp and Meta against NSO Group in US court.²⁹ It provides the most detailed view yet into the inner workings of the Pegasus spyware system. This includes confirmation of key technical capabilities such as the infection vectors and methodologies used to infect devices, supported by analysis of internal NSO Group documents, that until now had only been identified via forensic investigations. It also presents new material that validates the accuracy and significance of the dataset underpinning the original 2021 Pegasus Project investigation. Finally, this research provides an updated analysis, drawing on previously published Pegasus forensic evidence and

²⁸ A version of this chapter was originally published on in July 2026. Amnesty International Security Lab, *Inside Pegasus: the evolution of the world's most notorious spyware system*, 16 July 2026, <https://securitylab.amnesty.org/latest/2026/07/inside-pegasus-the-evolution-of-the-worlds-most-notorious-spyware/>

²⁹ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, <https://www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/> (accessed on 16 July 2026). Amnesty International's Security Lab has created a repository of the key documents cited in the case on GitHub, in the interest of making this important material more accessible for all researchers and advocates working on spyware accountability efforts. Amnesty International, 'Inside Pegasus: key documents from WhatsApp v. NSO Group', 16 July 2026. <https://github.com/AmnestyTech/inside-pegasus> Every file in the repository is an extract from documents filed on the public court docket. Each page carries the court's filing stamp (Case 4:19-cv-07123-PJH ... Filed ...) and the parties' Bates numbers (NSO_WHATSAPP_..., WA-NSO...), so any extract can be traced back to its source filing and page. All documents in this repository are now in the public domain as public court exhibits. Some carry a "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" stamp. That was their designation during the litigation, before the court ordered them filed publicly; the stamp is a record of that history and has no bearing on their status now. All references in this chapter are made to the Amnesty International repository, for ease of reference.

newly released materials, to validate the technical methodology used to forensically link Pegasus spyware attacks targeting different victims as originating from the same Pegasus customer.

A key aim of this publication is to document and demystify the functionality and operations of technological systems like Pegasus, and to inform the wider spyware accountability community on how complex surveillance systems such as Pegasus are used by government customers. Public understanding of how such spyware systems operate is of critical value to technologists, researchers, and policy makers and others with an interest in understanding the targeted surveillance ecosystem and threats posed to human rights by surveillance technologies.

4.1 THE PEGASUS INFECTION PROCESS FROM THE ATTACKER PERSPECTIVE

Pegasus is sold to governments as an “end-to-end” cyber-intelligence solution. NSO Group is responsible for building and integrating the various technical components needed to perform spyware attacks, including creating exploits and infection vectors, deploying and monitoring anonymization servers, and designing a user interface which allows the ultimate end-user – a government customer³⁰ – to perform highly technically sophisticated attacks with little need for technical capabilities of their own.

Key components of the system, including the Pegasus user dashboard and the storage servers which archive surveillance data gathered from a victim’s device, are installed locally in the customer country, often in a server room at the customer site or headquarters.

However, other important components of the Pegasus system, particularly those used to send attacks and securely transfer the surveillance data from infected devices, are run and managed by NSO Group.

To keep attacks from being traced back to the customer, NSO Group operates much of the delivery and relay infrastructure in an anonymized fashion. In NSO’s own terminology, this is referred to as “whitened” infrastructure. A dedicated NSO team, “White Services”, is responsible for acquiring this infrastructure while aiming to prevent any attributable connection to NSO Group or the Pegasus customer. Much of the server infrastructure appears to be paid for with cryptocurrencies in order to achieve that goal.³¹ To avoid cross-contamination, NSO Group builds separate independent infrastructure and accounts for each customer, where technically feasible.

Anonymizing Network

The ATN is built from anonymized connectivity nodes spread over worldwide locations; they enable agent connections to be directed along varying paths before reaching the Pegasus servers. Anonymized nodes serve only a single client who can choose to manage their setup.

See Section 7.3 Anonymizing Transmission Network for more information.



“Anonymized nodes serve only a single client”³²

The NSO Group ‘managed services’ fall into two key categories: the anonymizing server and relay network, and the “whitened” accounts used to send exploits and interact with external service providers (such as SMS messaging services).

The first category includes what NSO Group has termed the “Pegasus Anonymizing Transmission Network”,³³ which is the custom VPN network used to hide the location and actions taken by the Pegasus customer system. It is used to send the spyware payload to the target device, and to forward collected

³⁰ NSO Group state that their products are sold only to government agencies: “NSO Group licenses its products only to government intelligence and law enforcement agencies for the sole purpose of preventing and investigating terror and serious crime”. NSO Group, Governance, <https://www.nsoigroup.com/governance/> (accessed on 26 July 2026).

³¹ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Video Deposition of Ramon Eshkar, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/testimony/eshkar-deposition.pdf>, p. 84.

³² District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, August 2018, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/products-and-capabilities/pegasus-product-description-2018.pdf>, p. 14.

³³ ‘Pegasus Product Description’. Available at: <https://embed.documentcloud.org/documents/4599753-NSO-Pegasus/>, p. 17 (accessed on 16 July 2026).

surveillance data back to the customer's on-site system, arranged so that neither the target nor an investigator can readily identify the customer or the wider Pegasus network behind it.

The second category, examined later in this report, includes the individual attack accounts, infection domains and servers used against a customer's targets. The "White Services" department creates, as a standard practice, fresh, customer-specific accounts and domain names for each customer.³⁴ This practice aligns with the Security Lab's own forensic observations that a given account or domain is only found on target devices which could plausibly have been targeted by the same customer. This crucial observation, now confirmed by NSO Group documentation, allows attacks to be reliably clustered and attributed based on forensic evidence.

Due to the complex technical nature of the spyware system and network, NSO Group maintains a Network Operation Center ("NOC") responsible for monitoring customer systems for technical faults and/or operational security alerts. Customer-facing documents state that while NSO Group's support staff and the NOC "can see security alerts, they cannot view any collected target or operational-related data".³⁵ This real-time monitoring capability suggests that NSO Group must receive some level of telemetry or alerts from customer systems, necessary to detect failed or exposed infection attempts.

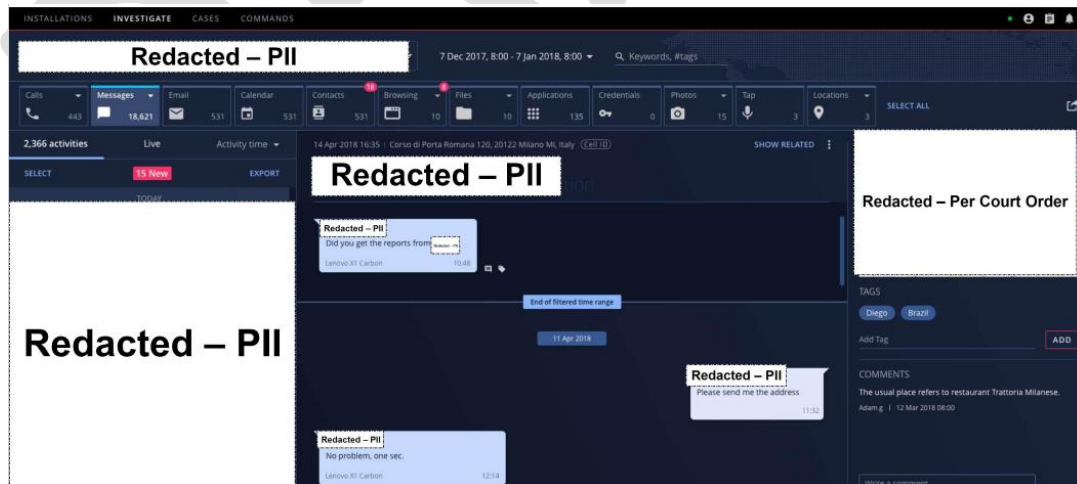
Note: Our 24/7 Support Center monitors security alerts arriving from all client systems; however, while the Support Center can see security alerts, they cannot view any collected target or operational-related data. Should there be a security incident, the client must immediately follow Support Center guidance and directions.



24/7 Support Center monitors security³⁶

4.1.1 THE PEGASUS DASHBOARD: USERS, GROUPS, AND CASES

Central to the customer's use of the spyware is the Pegasus dashboard. It allows the spyware operators, working for NSO's government customers, to manage and interact with all key aspects of the system, including launching new spyware infections and analysing the retrieved surveillance data.



The Pegasus 3 Dashboard³⁷

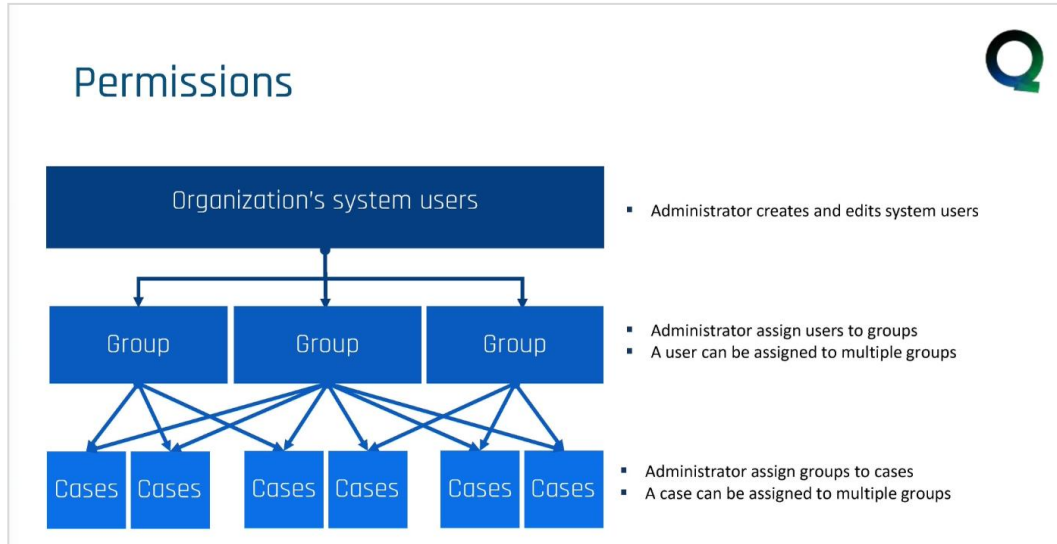
³⁴ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Eshkar transcripts, https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/testimony/WhatsApp-v-NSO-Eshkar-Transcripts_Case-4-19-cv-07123-PJH.pdf, pp. 2-11.

³⁵ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/products-and-capabilities/pegasus-product-description-2018.pdf>, p. 22.

³⁶ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, (previously cited), p. 22.

³⁷ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/products-and-capabilities/pegasus-3-introduction.pdf>, p. 25.

NSO Group provides the Pegasus dashboard as a user-friendly browser-based console, only accessible locally on the government customer's premises. The system is built with confidentiality in mind. The system distinguishes multiple roles for each individual user account, such as *analyst*, *operator*, *supervisor*, and *administrator*.



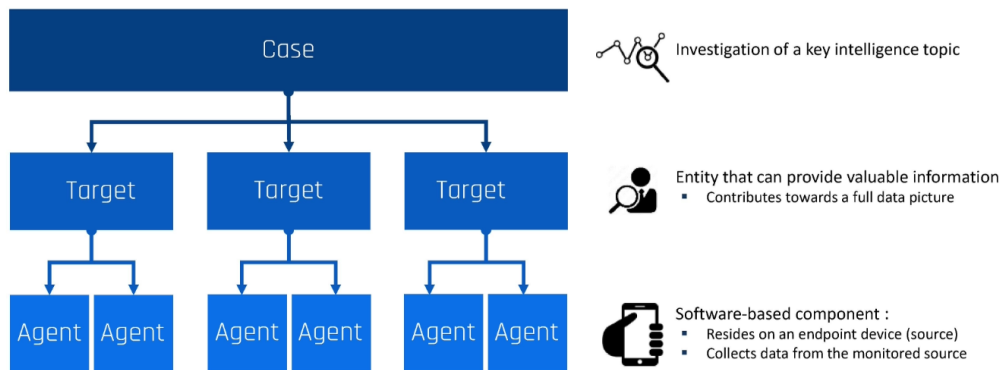
Tiered permissions limiting case visibility by user and group³⁸

Any surveillance operation using Pegasus is managed and controlled inside “groups” and “cases”. System administrators or other individuals on the customer-side with supervisor privileges can assign specific individuals, termed “analysts”, to one or more groups. Groups are used to manage system permissions for analysts, determining which cases they have access to. Once assigned to groups and cases, analysts gain the ability to view gathered surveillance records and, depending on system permissions, to launch new surveillance operations. This layered permissions system means access to case information is tightly restricted on the customer side and on a need-to-know basis. Individual analysts are only able to see their assigned cases and do not have visibility into how the overall system is being used. Individual analysts and cases can be assigned to more than one group.

³⁸ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction, (previously cited), p. 29.

Mission hierarchies

Users are granted permissions based on their cases



A case organizes targets around a key intelligence topic³⁹

Targeting in the Pegasus system begins with the opening of a “case”. A case is used to “organize and manage targets” and can be used to group intelligence-gathering efforts around a “key intelligence topic” such as a particular organization or a particular investigation.⁴⁰ Multiple individual targets can be added inside a single “case”.

4.1.2 LAUNCHING A PEGASUS ATTACK: TARGET SELECTION, DEVICE FINGERPRINTING, AND VECTOR DELIVERY

Once the case is created, the spyware operator (the person using the Pegasus system) can add new prospective spyware targets to the case. For each target, the operator can enter one or more phone numbers. The target phone number is the primary identifier used in the Pegasus system. The phone number is often all that is needed to perform an attack.

Pegasus training material describes situations where it may not be possible to attack a target directly, for example, if they do not use a smartphone or are highly security-conscious in how they use their device. In those circumstances, NSO Group suggests expanding to “close-circle infection”, targeting others connected to the target, potentially including colleagues, friends or family members of the primary target in order to gather information about them indirectly.

Pegasus use has previously been documented against the family members⁴¹ of political opposition members and journalists, including some who were children⁴² when they were targeted.

³⁹ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction, (previously cited), p. 15.

⁴⁰ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction’ (previously cited), p. 22.

⁴¹ Guardian, “Hotel Rwanda activist’s daughter placed under Pegasus surveillance”, 19 July 2021, <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>

⁴² Citizen Lab, “Reckless exploit: Mexican journalists, lawyers and a child targeted with NSO spyware”, 19 June 2017, <https://citizenlab.ca/research/reckless-exploit-mexico-nso/>

But, what happens if

- Target does not use a smartphone
- Target frequently changes his phone
- Target's phone number is unknown
- Target is highly aware and alert



Close-circle infection



*Close-circle infection*⁴³

Once the target phone number is added, the Pegasus system will then perform “fingerprinting” steps to determine critical information about the target device. This verification step is needed before an attack can be launched. The fingerprinting step includes checking:

1. if the target phone number is attached to a smartphone (rather than another type of device),
2. if the phone runs Android or iOS,
3. if the phone is currently switched on and connected to the mobile network,
4. the phone's current network,
5. if the phone is roaming in another country, and
6. which apps are installed on the device (such as WhatsApp or iMessage).

This fingerprinting process occurs only after the target phone number has been entered by the Pegasus operator as a potential target. As this process can require active probes being sent to the target device and network, it has the potential to leave forensic traces in various locations, such as in logs of which messenger accounts have tried communicating with a device.

When referring to Pegasus Project records, Amnesty International uses the terminology *selected* or *selected for targeting* to refer to phone numbers entered in the Pegasus system as potential targets. Being entered in the system and *selected* as a target already shows the intention of the Pegasus operator to carry out covert surveillance on the target device, whether or not it was ultimately infected.

⁴³ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction, (previously cited), p. 29.

3 Mobile Device Installations

The heart of any endpoint-based intelligence operation is installing a mobile endpoint on a target's device—each installation is carefully planned to ensure success.

The solution supports installation methods and capabilities that satisfy various operational scenarios. The following sections describe the different endpoint installation tools and techniques that are provided by the system.

The solution has worldwide global coverage and is MNO independent.

3.1 OS Detection

Due to the system's vast intelligence collection capabilities, certain intelligence pieces can be collected even prior to successful installation, and some of them can serve the operator's efforts to maximize the installation success rate. The operating system (OS) detection capability helps the operator decide which installation vector to use. The system will suggest the most effective and secure installation vector for the designated OS and thus help the operator overcome the multi front battle of the diverse mobile market.

3.2 Installation Vector Selection

Once the operator identifies the target's OS, they can select one of the system's multiple installation vectors.

The system will automatically suggest the most efficient and secure vector to match the current conditions, but the operator can override this suggestion and choose a different vector to suit the operational needs.

The system offers multiple vectors which require minimal user interaction—requiring no more than a single click.

3.2.1 Social Engineering

As targets today are extremely security-aware and no longer naive, special precautions must be taken to ensure the safety of an operation.

The solution offers tools for composing tailored, yet innocent looking messages—this is crucial as content credibility greatly affects whether a target clicks a link. The messages are designed to be sent at different times through various channels.

3.3 Installation Progress Tracking

During the installation process, the operator can keep track of the endpoint's installation status, to understand exactly what the status of each installation stage is and be in control on the entire operation. By viewing a clear status of the installation progress, the system operator can ultimately plan the operation.



Validation steps the system performs before launching an attack⁴⁴

The fingerprinting results help the Pegasus system, and the spyware operator using it, to determine if they have a viable opportunity to attempt infecting the device, and if so, which “installation vector” (exploit) should be used against the target. NSO Group internal material appears to use the term “vector” broadly, referring at times to a particular exploit, and other times to a broader capability (i.e. zero-click targeting WhatsApp). We will similarly use “vector” to refer both to the attack technique and to specific exploits.

⁴⁴ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Mobile Endpoint – Product Description, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/products-and-capabilities/mobile-endpoint-product-description.pdf>, p. 46.

Each Pegasus deployment is bound by licensing restrictions on the customer side, including the number of unique targets, the number of simultaneous infections and the countries that may be targeted. The country code of the target's number and the phone's current location are checked against these terms before an infection can proceed. Certain countries, such as the United States and Israel, are barred for most customers. However, this is a policy rather than a technical limitation, and NSO Group has indicated that customers based in those countries could be provided the capability to infect local numbers. There are also likely exceptions for NSO Group-managed systems used to perform demonstrations of the product for potential customers, as will be seen later in this report.

The list of permitted countries can change over time, and a customer may license additional countries subject to approval by NSO Group and most likely the relevant export authority.

4.1.3 THE PEGASUS INFECTION PROCESS

Pegasus supports a range of exploits (malicious code used to gain access to a target) and infection techniques (termed “vectors” by NSO Group). The set of supported vectors is constantly evolving as new vectors get developed by NSO Group and exploits get patched by device vendors or otherwise stop working. These are broadly divided into zero-click (“Covert”) or 1-click (“Triggered”) vectors, defined by the user-interaction required for the infection process to succeed. Section 3 (“The evolution of Pegasus Infection Vectors”) reviews what is known about Pegasus infection vectors in more depth.

Once the operator approves the infection attempt (“Installation”), the Pegasus system will begin carrying out the spyware infection process in the background. The operator can monitor the stages of the infection attempt and will get a notification if the spyware agent is successfully installed on the device, or if it fails for some reason.

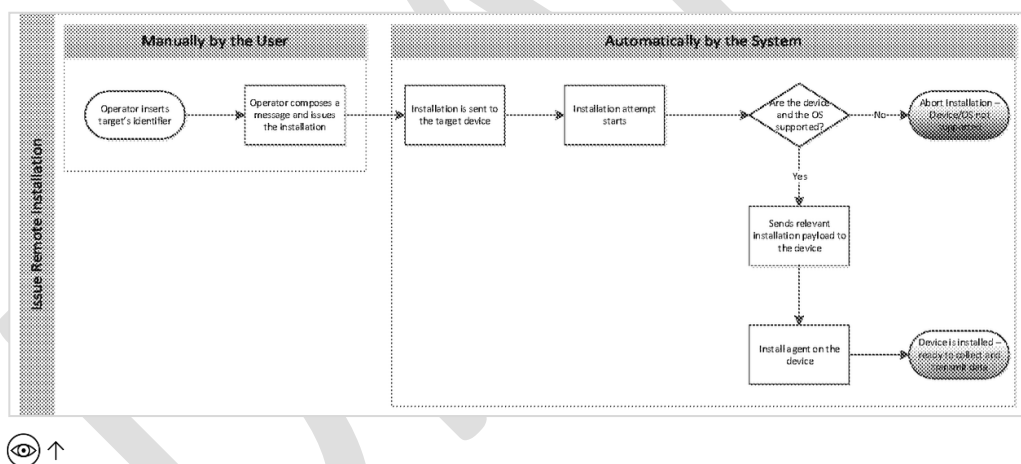


Diagram showing manual steps triggered by the operator, and automatic steps managed by the system⁴⁵

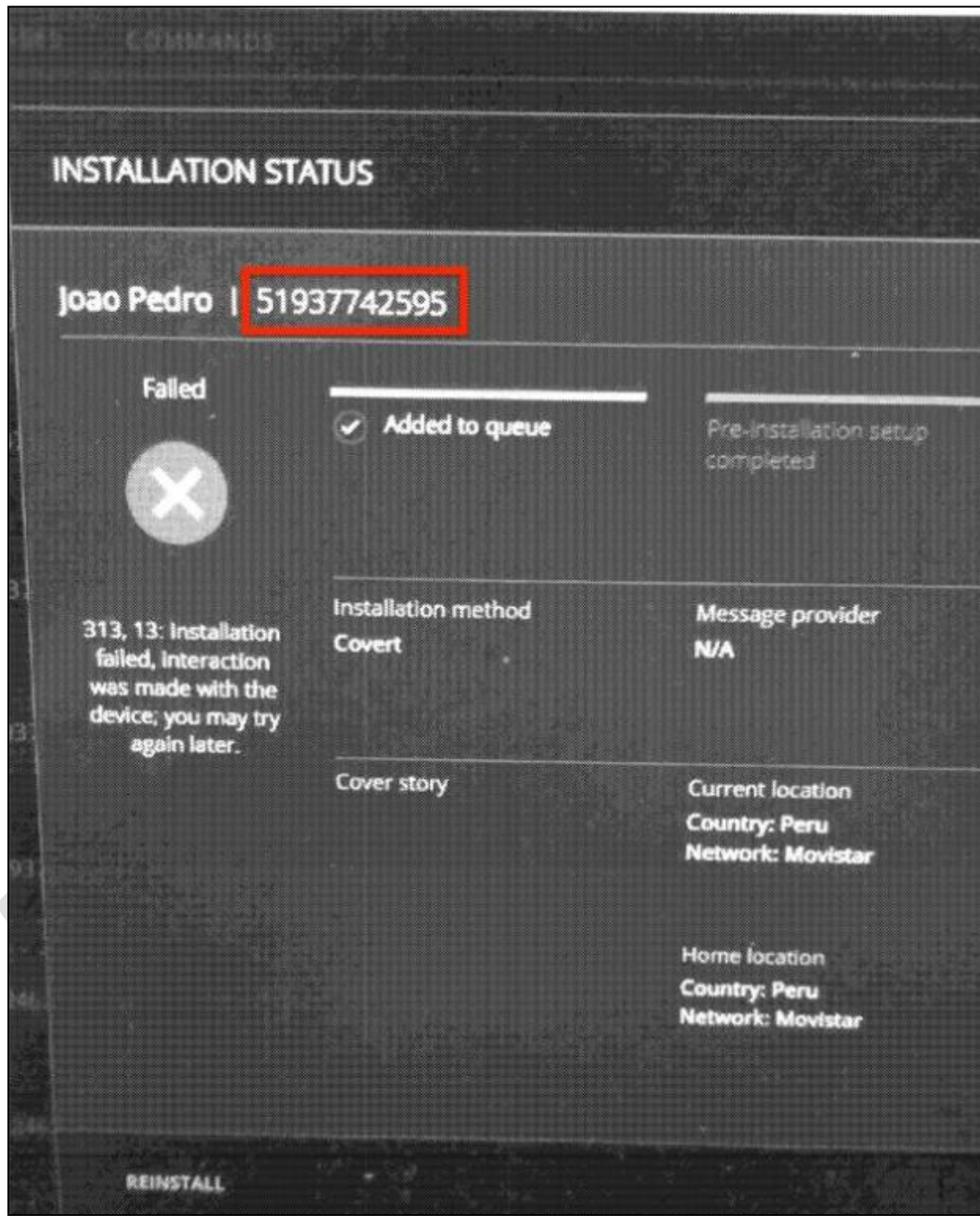
Documents from the WhatsApp court case include a screenshot of a failed Pegasus infection attempt which provides further details about the infection process. The status page (shown below) shows the home mobile operator and current network of the target's phone number, information likely derived from a Home Location Register (HLR) lookup. An HLR lookup reveals which network or country a mobile subscriber is currently connected to, without alerting the subscriber. A separate internal NSO Group document indicates that HLR lookups are an integrated part of the target validation process.⁴⁶

The screenshot also shows that the selected installation method was “Covert” (zero-click) and, as such, did not require use of an SMS message provider or a social engineering cover story. Additionally, the failure message says “interaction was made with the device; you may try again later”, showing that failed infection attempts could also result in forensic traces being left on a device. Internal design documents show NSO

⁴⁵ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, (previously cited), p. 14.

⁴⁶ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pitch: Happy Flow, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/business-and-customers/pitch-happy-flow.pdf>, p. 95.

Group explicitly addressing and documenting device interactions and other operational security risks when designing new infection vectors.



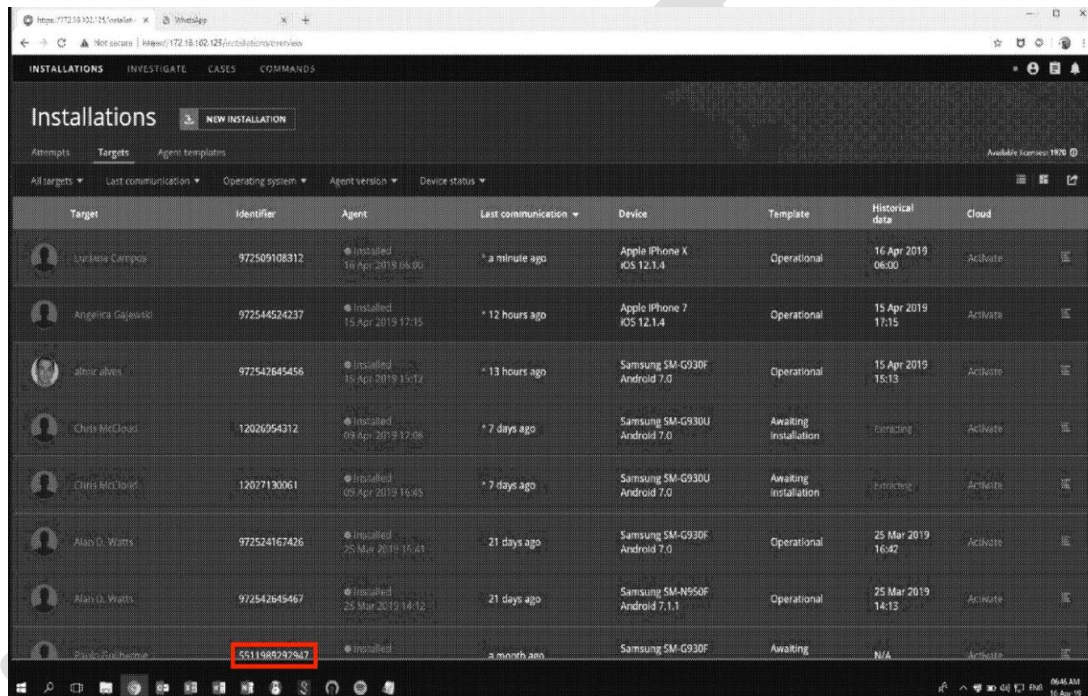
Error message showing a failed "Covert" (zero-click) infection attempt⁴⁷

Other operational security and targeting restrictions also apply to protect the customer and NSO Group from exposure, including limiting how often the same person can be targeted, and the wait period between subsequent targeting attempts. These operational security restrictions differ between vectors and NSO Group

⁴⁷ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Expert report of Anthony Vance, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/testimony/vance-expert-report.pdf>, p. 13.

appears to maintain a system called “Abuse Prevention” to manage these restrictions for customers.⁴⁸ Spyware operators may want to test the system and ensure a vector is correctly configured before launching it against an important target. This appears to have been common practice. An NSO Group employee described in court testimony that the Pegasus system had a “whitelist” feature to allow repeated test infections, without any wait period restrictions, against one or more testing devices in the possession of the customer.⁴⁹ These show that customers may perform test infections as part of normal usage of Pegasus system.

Such repeated infection attempts would otherwise be blocked for operational security reasons. This testing activity would result in the operator or operator-controlled phone numbers being *selected* as target phone numbers, and being recorded in logs created by the Pegasus system. As a result, investigations drawing on Pegasus Project targeting records have been able to identify suspected spyware operator-owned phone numbers *selected* in multiple countries, likely for testing purposes.



The screenshot shows a web interface titled 'Installations' with tabs for 'Attempts', 'Targets', and 'Agent templates'. The 'Targets' tab is active, displaying a table of installed agents. The table has columns for Target, Identifier, Agent, Last communication, Device, Template, Historical data, and Cloud. One identifier, '5511985292547', is highlighted with a red box.

Target	Identifier	Agent	Last communication	Device	Template	Historical data	Cloud
Lurdesse Campos	972509108312	Installed 16 Apr 2019 16:00	* a minute ago	Apple iPhone X iOS 12.1.4	Operational	16 Apr 2019 06:00	Activate
Angelica Gajowski	972546524237	Installed 15 Apr 2019 17:15	* 12 hours ago	Apple iPhone 7 iOS 12.1.4	Operational	15 Apr 2019 17:15	Activate
almir alves	972542645456	Installed 15 Apr 2019 15:12	* 13 hours ago	Samsung SM-G930F Android 7.0	Operational	15 Apr 2019 15:13	Activate
Chris McCloud	12026054312	Installed 09 Apr 2019 17:06	* 7 days ago	Samsung SM-G930U Android 7.0	Awaiting installation	Extracting	Activate
Chris McCloud	12027130061	Installed 09 Apr 2019 16:45	* 7 days ago	Samsung SM-G930U Android 7.0	Awaiting installation	Extracting	Activate
Alan O. Watts	972524167426	Installed 25 Mar 2019 16:41	21 days ago	Samsung SM-G930F Android 7.0	Operational	25 Mar 2019 16:42	Activate
Alan O. Watts	972542645467	Installed 25 Mar 2019 14:12	21 days ago	Samsung SM-N950F Android 7.1.1	Operational	25 Mar 2019 14:13	Activate
Paulo Guilherme	5511985292547	Installed	a month ago	Samsung SM-G930F	Awaiting	N/A	Activate

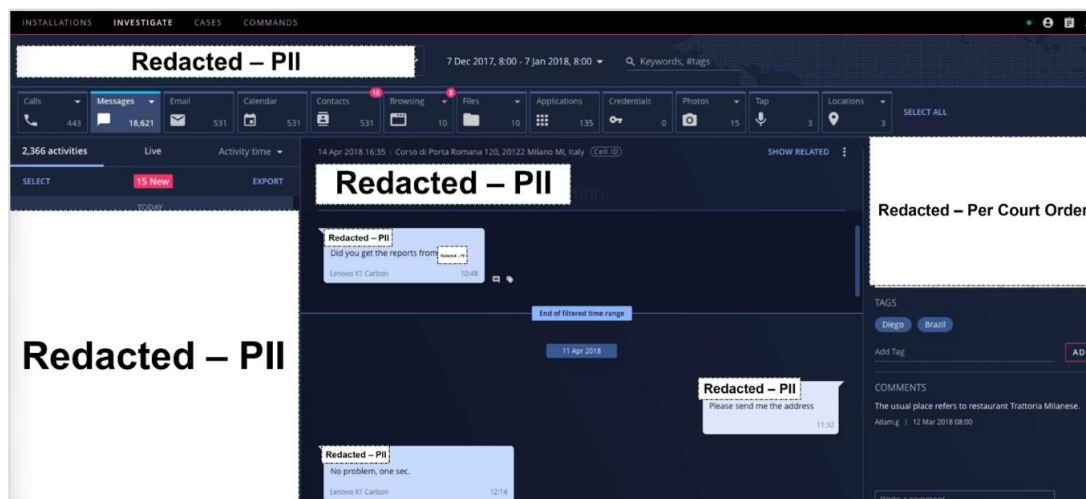
 Demo Pegasus interface showing the status of various installation attempts⁵⁰

After a successful installation, the operation moves from targeting to collection. The “Investigate” area of the dashboard (second tab seen in the top left corner of the image above) lets the operator view and manage all data exfiltrated from the compromised devices. For each compromised device, the data is organized by data type, including calls, messages, email, calendar, contacts, browsing, files, applications, and photos.

⁴⁸ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Opsec Rule Engine - PRD, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/operations-and-opsec/opsec-rule-engine-prd.pdf>, p. 14.

⁴⁹ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Video Deposition of Ramon Eshkar, (previously cited), p. 82.

⁵⁰ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Expert report of Anthony Vance, (previously cited), p. 15.



Pegasus interface shown to operator after successful infection of a target⁵¹

Notably, the system also presents a “credentials” tab, likely containing saved passwords, authentication tokens and other credentials gathered from the victim’s device.

Access to these stolen credentials provides an opportunity for the Pegasus operator to gain and maintain access to sensitive online accounts of the victim, even when the mobile device itself is no longer infected. Indeed, partial redacted documentation from a 2018 Pegasus product description explicitly talks about the power of data accessible from cloud accounts: “Cloud brings in a continual flow of information that can last months at a time”.

3.2

Redacted – Export Controlled

Data Collection

Data is securely extracted from clouds—there is no impact, whatsoever, on the behavior of device applications and user accounts.

Data stored on mobile devices merely hints at the mass of available historical information—dating back months and even years—that can be retrieved. Cloud brings in a continual flow of information that can last months at a time.

Newly generated information is securely transmitted to the Pegasus system.

- Instant messaging	- Email
- Location history	- Browsing history
- Account backups	- File-sharing storage

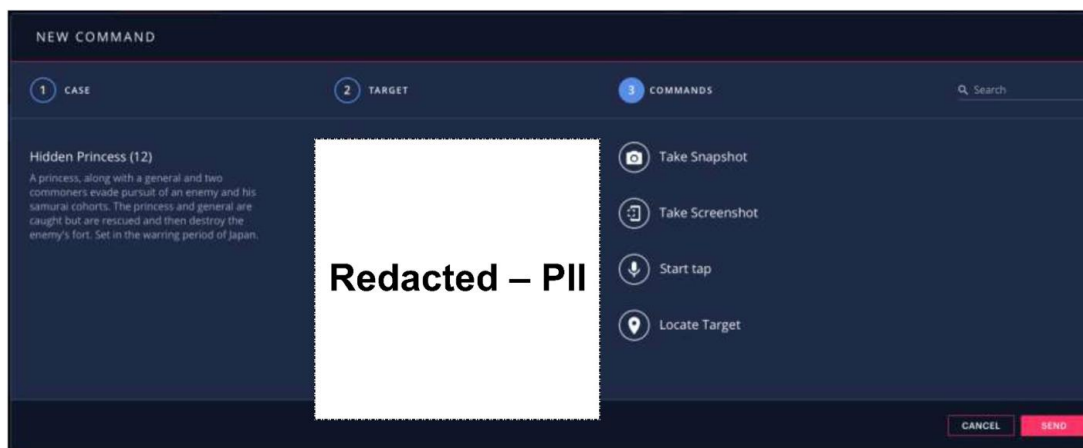


Description of Pegasus data collection capabilities from cloud accounts⁵²

⁵¹ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction, (previously cited), p. 25.

⁵² District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, (previously cited), p. 12.

In addition to providing access to collected surveillance data, the Pegasus dashboard also allows the spyware operation to queue up new actions (“Commands”) to be performed on the infected target device. In the image below, the “Commands” module allows active commands to be sent to one or more targets in a group, including to take photos using the phone’s camera, turn on the phone’s microphone or report the location of the target. Other documents indicate that such active steps (“recording from the microphone”) can be pre-scheduled and run automatically when the target is known to have an important meeting scheduled in their calendar.



Pegasus commands module allowing for manual action to be launched on the target device.⁵³

The newly public NSO Group material provides valuable new evidence on internals and capabilities of a sophisticated mercenary spyware product. The documents confirm and validate years of civil society research on the operations and functionality of the Pegasus spyware. They also provide new and important visibility into the workflow and exact methodology used by customers of the Pegasus spyware to target and infect devices.

4.1.4 NEW MATERIAL FURTHER VALIDATES SIGNIFICANCE OF PEGASUS PROJECT LEAK

As part of the 2021 Pegasus Project,⁵⁴ Amnesty International had access to a leaked database of phone numbers *selected* as potential Pegasus targets by NSO Group customers around the world. Numerous individuals, whose phone numbers appear in the original leak, have later been forensically confirmed to have been infected with Pegasus, by many different Pegasus customers.⁵⁵

The underlying dataset is clearly divided into distinct groups of phone numbers which, in most cases, map directly to a specific Pegasus customer or customer system. This allows for a presumptive attribution based on the geographical scope and individual targets selected in each group. For ease of reference, we will refer to the distinct groups of targeted phone numbers as “clusters” rather than “customers” or “operators” because not all groups map directly to specific production customers.

Some of these target groups or “clusters”, as will be shown, appear to tie directly to internal NSO Group controlled Pegasus systems used when performing pre-sales demos of the Pegasus system for potential clients given the evidence in the WhatsApp filings. Another cluster appears to have been used for internal

⁵³ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 3 – Introduction, (previously cited), p. 27.

⁵⁴ Amnesty International Security Lab, Case study: The Pegasus Project, (previously cited).

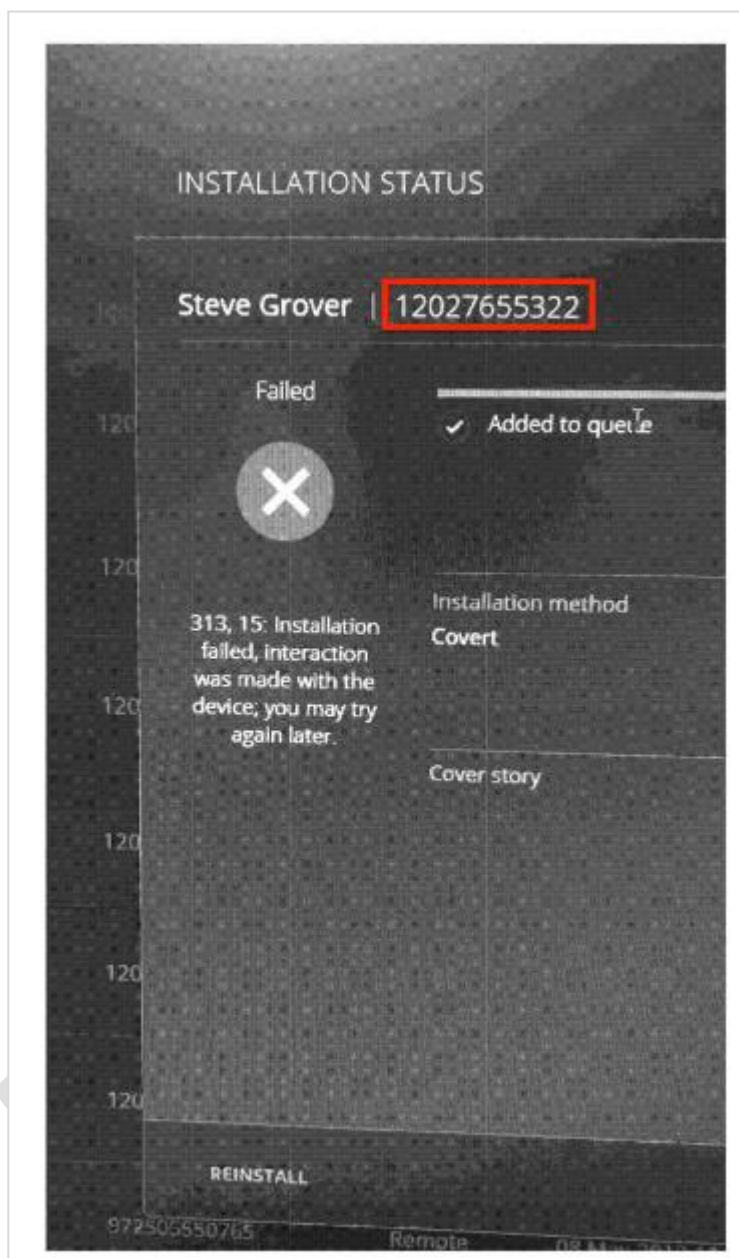
⁵⁵ Amnesty International, *Forensic Methodology Report: How to catch NSO Group’s Pegasus*, 18 July 2021, <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

testing within NSO group, with phone numbers associated with multiple NSO Group staff members appearing in that cluster.

Two of the clusters in the original Pegasus Project leak map directly to a Pegasus deployment which NSO Group internally refer to as “Sales 3” and “Sales 6”, identified in the documents from the WhatsApp court case. A screenshot of a Pegasus dashboard included in the WhatsApp filings shows numerous apparent test infections targeting numbers in various countries in 2019 including Israel, Peru, Brazil and the United States.⁵⁶ Many of these same phone numbers also appear in the Pegasus Project cluster which we infer is tied to “Sales 3” system.

Additionally, a US phone number “+12027655322” – which WhatsApp court-filings indicate was used by an NSO Group sales representative – was repeatedly *selected for targeting* in two Pegasus Project clusters corresponding to NSO Group’s “Sales 3” and “Sales 6” systems. Pegasus Project records show the phone number was selected for targeting again on 9 May 2019, the same day that the NSO Group representative sent a screenshot of a failed infection attempt targeting that phone number to NSO Group’s Network Operations Center (NOC).

⁵⁶ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Expert report of Anthony Vance, (previously cited), p. 15.



Installation status panel for Pegasus on the phone number +12027655322.⁵⁷

The same witness document filled by WhatsApp also includes an infection attempt in May 2019 targeting a Peruvian phone number “+51937742595”, again apparently as part of a demonstration. The Pegasus Project records again show the same Peruvian phone number was selected on 7 May 2019 in the two clusters associated with NSO Group’s “Sales 3” and Sales 6” Pegasus deployments.

⁵⁷ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Expert report of Anthony Vance, (previously cited), p. 10.



Installation status panel for Pegasus on the phone number +51937742595.⁵⁸

In sum, the newly disclosed WhatsApp material provides a further, independent verification of the evidentiary value of the Pegasus Project dataset. The dataset repeatedly records phone numbers belonging to NSO Group employees, falling within clusters that correspond to internal Pegasus deployments used for software testing and pre-sales demonstrations, including two which NSO Group internally labels "Sales 3" and "Sales 6". This close correspondence between infection attempts carried out on NSO Group-managed Pegasus systems and Pegasus Project records, demonstrates that the Pegasus Project data reflects and corresponds with genuine activity on Pegasus systems. It stands in direct contradiction to NSO Group's repeated position that "we still do not see any correlation of these lists to anything related to use of NSO Group technologies".⁵⁹

The Pegasus Project records are highly consistent with the findings of Amnesty International's independent forensic investigations. Individuals whose devices we have forensically confirmed as targeted and infected with Pegasus reappear in the Pegasus Project records as targets of one specific Pegasus customer system.

⁵⁸ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Expert report of Anthony Vance, (previously cited), p. 13.

⁵⁹ Guardian, "Response from NSO and governments", 18 July 2021, <https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments>

In these cases, the victim's phone number was frequently selected, or re-selected, shortly before an infection attempt was carried out, as evidenced by the WhatsApp filings.

NSO Group maintained standalone Pegasus systems used to test features and to perform product demonstrations for potential or existing clients, including the DSGT. Between 17 December and 19 December 2018, two Moroccan phone numbers were entered repeatedly into one of these separate NSO Group-controlled sales demo Pegasus systems. This followed WhatsApp implementing a server-side block for the initial Heaven WhatsApp vector on 5 December 2018. This suggests that NSO Group was actively testing functionality or demonstrating new Pegasus features at this time. The same demo numbers were later selected in the Morocco customer system on 24 December 2018 and 17 January 2019.

4.2 EVOLUTION OF PEGASUS INFECTION VECTORS

Internal NSO Group documentation and marketing material describe the evolving set of infection vectors (exploits and infection techniques) offered to customers over time, from targeting BlackBerry devices as seen in an early 2013 brochure, to developing advanced attacks targeting iPhones. Broadly, these include Triggered (1-click), Covert (zero-click), Tactical Network Element (“Network injection via MiTM”), and Inline (network injection), and “Physical”, where the operator has physical access to the device. One redacted methodology most likely refers to infection of a device over radio interfaces (such as WiFi or Bluetooth) when “within range” of the target device.⁶⁰

4.1 Remote Installation (Unlimited range)

Remote installations include both covert and social-engineering methodologies. The Pegasus solution offers many tools for composing tailored, yet innocent-looking messages—this is crucial as content credibility greatly affects whether or not a target will click a link.

Using the below methods, only a target's phone number (MSISDN) is required for a successful installation.

Covert

1. A covert message is sent to a mobile device; the target is not engaged—there is no need to click a link or open a message.
2. The message causes the smartphone to download and install the agent—the device shows no signs of change or interference.
3. The installation is completely invisible.

The Pegasus system's unique, remote installation capability gives our solution a vast advantage over other offerings found in the market.

- Covert installation process is invisible to the target and doesn't require their engagement.
- System is MNO independent.
- Activation is handled from a command and control center.
- Solution has an unlimited range and works using any MNO. Thus, the Pegasus agent can be installed on any supported device, anywhere in the world.

Triggered (Social Engineering)

System operators can choose a different approach and craft an SMS, instant message (IM), or email. This approach prompts a target to click on a message link.

- One click, whether active or unintentional, leads to an agent installation.
- The process is completely covert and there is absolutely no sign that software is being installed on their smartphone.



Excerpt from Pegasus product manual showing supported infection methodologies.⁶¹

Zero-click attacks are preferred in the system where available and supported for the target device. When a zero-click or “Covert” attack vector is not supported for a particular device, the system will suggest performing a “Triggered” infection. The Pegasus system can then aid the operator to craft and send a tailored social engineering message to attempt to infect the target.

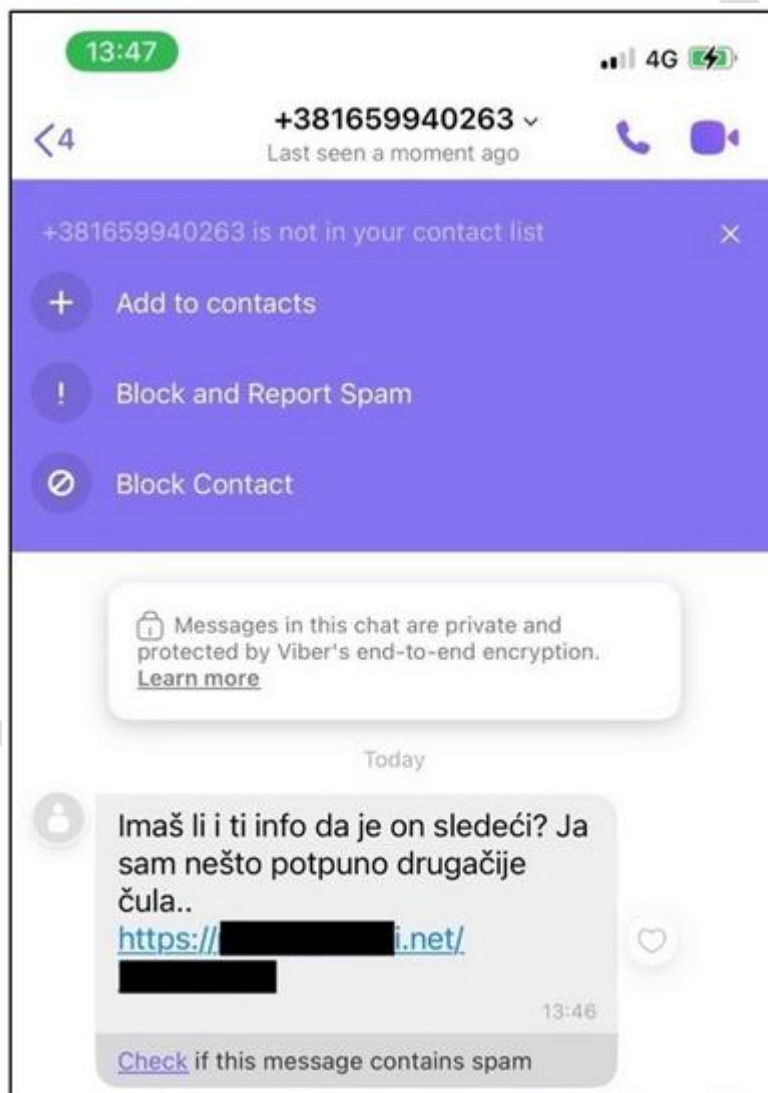
⁶⁰ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, (previously cited), p. 12.

⁶¹ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus version 3.0 – Product Description, (previously cited), p. 12.

The precise vector (or exploitation technique) is not necessarily revealed to the operator. Instead, the system proposes the best high-level approach based on the current system capabilities and the target's device, labelling it in broad terms such as "iOS Covert", "Android Covert" or "iOS Triggered".

The set of infection vectors supported by NSO Group has evolved over time due to the development of new capabilities and the changing set of devices and operating systems used by targets. Older NSO Group marketing material from 2013 describes capabilities to infect BlackBerry devices, which appears to have become less important as Android and iOS devices have come to dominate the mobile phone market.

Pegasus 1-click attacks require action from the target to enable the infection of their device, typically by opening a malicious link. Various social engineering techniques are used to trick the target into opening the link, including spoofing legitimate websites or news articles.



Screenshot of a Viber message containing a 1-click attack, received by the Serbian journalist "Bogdana" on her iPhone⁶²

If clicked on, the attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device. Amnesty International's Security Lab has detected 1-click Pegasus spyware attacks on multiple occasions, including in Serbia, Poland, India and Mexico, among others.

The same zero-day exploits which target web-browsers can also be used to perform a form of zero-interaction attack, if the Pegasus customer has the cooperation of the target's mobile operation. So-called

⁶² Amnesty International Security Lab, "Serbia: Journalists targeted with Pegasus spyware", 27 March 2025, <https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/>

network injection attacks use networking traffic manipulation to redirect a target's phone to a malicious spyware infection URL simply while the target is browsing the web.

4.2.1 INFECTION WITH ZERO-CLICK ATTACKS

Forensic investigations conducted prior to this technical research indicate that NSO Group had remote zero-click capabilities against iOS from at least 2017, and against most Android devices from early 2018.

These insights into NSO Group infection vectors gleaned from forensic investigations are now validated and significantly deepened by new NSO Group material disclosed as part of the WhatsApp case. Zero-click vectors targeting Android devices via WhatsApp were the only Covert/zero-click vector method in the 2018-2020 period, although the exact underlying exploit changed over this time. The expert report of Anthony Vance reproduces an internal NSO support document recording that “Pegasus 2.50 is officially approved for production. This version introduces: – Heaven – the first 0-clicks installation vector for Broad Android devices!”, and states that “Other installation attack vectors used by Pegasus/Phantom are ‘Eden’ and ‘Erised,’ and these and Heaven are referred to by the umbrella term ‘Hummingbird,’ all of which exploit WhatsApp in order to install Pegasus/Phantom”.⁶³ Heaven was first released for production use around January 2018.⁶⁴ The ERISED vector was delivered via WhatsApp but appears to have only been functional on Samsung devices. The Samsung-only exploit shows similarities to more recent in-the-wild Samsung zero-click exploits,⁶⁵ which used manipulated DNG files targeting the Quram library, an image parsing library specific to Samsung devices.

NSO Group also had multiple iOS vectors during that time, although the WhatsApp material is less detailed on these vectors. A zero-click vector “**Diablo**” was available in 2018 and likely corresponds to an exploit targeting iOS 11.X devices which has been observed forensically as targeting the Voice-over-WiFi implementation on iOS. A message from an NSO pre-sales engineer, put to Joshua Shaner at his deposition, lists the vector alongside Heaven: “Tomorrow at ten we'll have a demo in Israel for a potential client visit (Smart). Sales 4, one-click, Diablo and Heaven. Thanks.”⁶⁶ NSO Group later rolled out a new iOS 12.X vector “**Dragonfly**” which targeted via iMessage. The vector was used very actively throughout 2019 until the vector was likely inadvertently mitigated in iOS 12.4.1 in response to Google Project Zero research into the iMessage zero-click attack surface.⁶⁷

Previous forensic investigations by Amnesty International's Security Lab have found that NSO Group continued to deploy further iPhone zero-click exploits in 2020 and 2021 including an iOS 13 zero-click vector targeting Apple Photos, an iOS 13 zero-click exploit targeting iMessage (publicly termed KISMET) and the widely documented iOS 14 zero-click (publicly termed Megalodon/FORCEDENTRY).

4.3 FORENSIC ATTRIBUTION OF ATTACKS BASED ON CUSTOMER-SPECIFIC INDICATORS OF COMPROMISE

Testimony from NSO Group employees, published following the WhatsApp litigation, describes a dedicated team – the “White Services” department – responsible for anonymously registering the email addresses, WhatsApp accounts, servers and domains needed for Pegasus on behalf of each customer. The team set these up in a deliberately anonymized way, to shield the customer and the wider Pegasus infrastructure from discovery by the targets or researchers.⁶⁸

⁶³ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Expert report of Anthony Vance, (previously cited), p. 17.

⁶⁴ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Pegasus 2.50 Android release notes, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/releases-and-versions/pegasus-2.50-android-release-notes.pdf>, p. 13.

⁶⁵ Google Project Zero, *A look at an Android ITW DNG exploit*, 12 December 2025, <https://projectzero.google/2025/12/android-itw-dng.html>

⁶⁶ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Video deposition of Joshua Shaner, <https://github.com/AmnestyTech/inside-pegasus/blob/main/documents/testimony/shaner-deposition.pdf>, p. 129.

⁶⁷ Virus Bulletin, *Exploit archaeology: a forensic history of in-the-wild nso group exploits*, 28 September 2022, <https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Exploit-archaeology-a-forensic-history-of-in-the-wild-NSO-Group-exploits.pdf>

⁶⁸ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, Video Deposition of Ramon Eshkar, (previously cited), pp. 2-11.

The Pegasus zero-click vectors which target Apple devices will typically be configured by the operator with specially created “attack” accounts used to send exploits over Apple services like iMessage. Historically, NSO Group’s “White Services” (see Section 4.1) team has first created anonymous Google or Outlook email accounts, and later registered these accounts for use with iCloud to be used in Apple device targeting. This is why many of the malicious Apple accounts used for Pegasus attacks and detailed in this section are also Gmail addresses.

As discussed in Section 4.1, for operational security reasons, NSO Group prepares a distinct, isolated set of infrastructure for each customer. While this is intended to protect customers from exposure, it has also provided a key opportunity for the forensic attribution of observed Pegasus attacks to a specific Pegasus customer.

It is possible to use customer-specific indicators of compromise (IoCs), such as iCloud accounts used to send zero-click infection attempts, to forensically link (or *cluster*) multiple Pegasus infections as having been performed by the same Pegasus customer. The unique, per-customer assignment of a zero-click attack account is what allows attacks to be clustered and attributed: where the same iCloud account appears across multiple targets, those targets were selected by the same Pegasus customer. Phone numbers targeted by the same attack accounts have typically had a geographic or thematic link that suggests a common Pegasus operator. Other technical evidence, such as the timeline of attacks, reinforces the evidence that attack infrastructure is customer-specific. Across hundreds of cases, Amnesty International has never detected evidence to suggest a single attacker account or infection domain being used by more than one Pegasus customer.

Zero-click attack accounts are also understood to be created for use with a specific infection vector. Different WhatsApp accounts were created and used when a new variant of NSO Group’s WhatsApp zero-click was launched. Similarly, forensic analysis carried out by Amnesty International’s Security Lab has found different Apple accounts being used when a new iOS zero-click vector is deployed by the same customer.

In some instances, multiple Pegasus-linked malicious iCloud accounts were observed sending probes to a target phone over a number of minutes, likely indicative of the customer’s Pegasus system automatically testing different infection vectors to see which can be used to infect the device. Testimony from NSO Group employees indicates the choice of vector was made internally in the system, and was not a visible choice for the surveillance operator. This behaviour, where multiple Pegasus attacker accounts were used to probe the same target device, also allowed researchers to link the unique email accounts used for different vectors to the same customer.

4.4 HOW NEWLY DISCLOSED DOCUMENTS ENHANCE PUBLIC UNDERSTANDING OF PEGASUS SPYWARE

The internal NSO Group material disclosed in the WhatsApp litigation, supported and enhanced by Amnesty International Security Lab’s forensic investigations, provides the most complete picture to date of how the Pegasus system is built, operated and maintained. Three findings are particularly notable.

First, Pegasus is not a product that is operated autonomously by the government customer. NSO Group builds new exploits and infection vectors, registers and operates the “whitened” (anonymized) infrastructure used to deliver them, and runs a “Network Operation Center” to monitor key components of the system, including responding to security alerts raised by failed or potentially detected attack attempts. Every software update released by the companies selling mobile devices and managing their operating systems (such as Apple) can break infection vectors or techniques, requiring ongoing maintenance and support by NSO Group for any customer system to remain functional. The system cannot operate without NSO Group’s ongoing involvement.

Second, the newly disclosed documents independently corroborate the authenticity and accuracy of the leaked dataset foundational to the Pegasus Project. Two clusters of target phone numbers in the leaked Pegasus Project records link directly to two internal NSO Group-managed Pegasus deployments that NSO Group internally labels “Sales 3” and “Sales 6”, used for pre-sales demonstrations. Other clusters appear to be linked to a Pegasus system used for internal testing.

Test infection attempts shown in NSO Group’s own Pegasus dashboards appear in the Pegasus Project records with the same specific test phone numbers and matching targeting dates. As previously documented in the original Pegasus Project, the records also correspond closely with forensically confirmed infections against the same targeted devices and phone numbers. NSO Group has long claimed that the Pegasus

Project data bears no relation to its technology. The forensic evidence and confirmation with NSO Group's own testing of Pegasus show otherwise.

Third, NSO Group's "White Services" team registers unique attack infrastructure for each customer, including Apple IDs and their associated email addresses, domains and servers. Amnesty International has never observed a given attacker account or infection domain being used by more than one customer at any time. The accounts and domains recovered in forensic analysis therefore function as customer fingerprints. Where the same account or domain recurs across different victims, Amnesty International assesses that those victims were targeted by the same customer.

Evidence relating to the "White Services" team validates the methodology of the spyware accountability community in linking clusters of spyware attacks to the same operator. The same methodology has and continues to be invaluable for the further attribution of Pegasus spyware attacks to the responsible customer.

DRAFT

5. THE USE OF PEGASUS SPYWARE IN MOROCCO

“We never start with Pegasus. It's the monster's weapon.”

Safir

This chapter reviews the previously documented history of Pegasus surveillance abuses in Morocco and draws on new evidence to present a detailed case study of how one spyware tool can be used for both transnational repression and to crush civil society and critical voices in the country.

The chapter first draws primarily on prior forensic investigations carried out by Amnesty International and documented in various Amnesty International publications since 2019 (Section 5.1). These previous investigative findings are newly contextualised and interpreted to show the evolution of Morocco's use of Pegasus between 2017 and 2021.

Building on analysis of how Pegasus works (Chapter 4), this chapter also draws on unprecedented whistleblower testimony, leaked materials, open-source intelligence, and journalistic investigations to definitively attribute the organization, key operatives and the wider intelligence apparatus responsible for the unlawful, persistent, and widespread abuse of Pegasus in the previously documented cases (Section 5.2). Building on leaked targeting records analysed by Amnesty International, this chapter also reveals the full scope and intensity of the Moroccan authorities' abuse of Pegasus, both inside Morocco and abroad. Together, these findings provide an unprecedented insight into human rights abuses carried out by the Moroccan authorities using Pegasus.

5.1 HISTORY OF PEGASUS USE BY MOROCCAN AUTHORITIES

Since 2017, multiple investigations by Amnesty International have found forensic evidence of NSO Group's Pegasus spyware being used to conduct surveillance against human rights defenders, lawyers and journalists in Morocco.⁶⁹ The Moroccan government's unlawful surveillance using Pegasus spyware of

⁶⁹ Amnesty International, “Morocco: Human Rights Defenders Targeted with NSO Group's Spyware”, 10 October 2019, <https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/>; Amnesty International, “Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools”, 22 June 2020, <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>; Amnesty International, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, (previously cited); Amnesty International, *Forensic Methodology Report: Pegasus Forensic Traces per Target*, 18 July 2021, <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/>; Amnesty International, *Appendix E – Pegasus Forensic Traces per Target Identified in the Aftermath of the Pegasus Project Revelations*, 6 August 2021, <https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/>

human rights defenders in Morocco and Western Sahara continued until at least November 2021 when Aminatou Haidar, a Western Saharan human rights defender, was targeted.⁷⁰

As part of the 2021 Pegasus Project,⁷¹ Amnesty International had access to a leaked database of phone numbers *selected* as Pegasus targets by NSO Group customers around the world. This dataset includes extensive records related to the Moroccan Pegasus customer, the DGST, as detailed below.⁷² All cases of Pegasus abuse described in this report are tied to the customer system controlled and operated by the DGST.

Those Pegasus Project records are highly consistent with the findings of Amnesty International's independent forensic investigations. Individuals found to have been targeted and infected with Pegasus in Morocco reappear consistently in Pegasus Project records as targets of the DGST. The victims' phone numbers were often selected or (re-selected) shortly before an infection was carried out. The Pegasus Project evidence is cited where relevant to the forensic cases and individual victims being documented.

In 2021, following the Pegasus Project publication, the Moroccan authorities stated that they had "never acquired computer software to infiltrate communication devices" and denied that they had "infiltrated the phones of several national and international public figures and heads of international s through computer software."⁷³

No further evidence of Pegasus-aided surveillance was observed in Morocco after November 2021, indicating that the Moroccan Pegasus customer contract either ended or was suspended around this time. Israeli export authorities tightened rules on the export of spyware and other surveillance technologies around the same time, leading to a restriction in the number of countries where Israeli spyware and cybersurveillance products could be sold.⁷⁴

Media reports indicate that the Moroccan authorities appear to have reviewed products by other companies to identify an alternative. A 2023 report in Israeli newspaper Haaretz alleged that spyware vendor Quadream had agreed a deal with Morocco to replace the government's use of Pegasus; however, these reports say the deal was not approved by the Israeli defence exports regulator following the Pegasus Project revelations.⁷⁵

5.1.1 INFECTION WITH 1-CLICK LINKS

In October 2019, Amnesty International forensically confirmed the first Pegasus infection attempts against Moroccan civil society, with the targeting in October 2017 of Abdessadak El Bouchattaoui, a human rights lawyer involved in the legal defence of protesters in the Hirak El-Rif movement, a series of demonstrations organized in the Rif region of northern Morocco in 2016 and 2017.⁷⁶ Therefore, the Moroccan use of Pegasus spyware appears to have been fully operational by October 2017.

Abdessadak El Bouchattaoui was first sent confirmed Pegasus 1-click links by SMS on 23 October 2017. Pegasus Project records show that his phone number was first entered into the Moroccan Pegasus system on 19 September 2017. His number was then *selected* on multiple occasions over the following year, including on 23 October 2017, shortly before he received an SMS infection link. The links included the **stopmsl.biz** domain, which Amnesty International confirmed was registered by NSO Group on 11 October 2017.

⁷⁰ Amnesty International Security Lab, "Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence", 9 March 2022, <https://securitylab.amnesty.org/latest/2022/03/morocco-western-sahara-activist-nso-pegasus/>

⁷¹ Amnesty International, "Pegasus Project: Apple iPhones compromised by NSO spyware", 19 July 2021, <https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/>

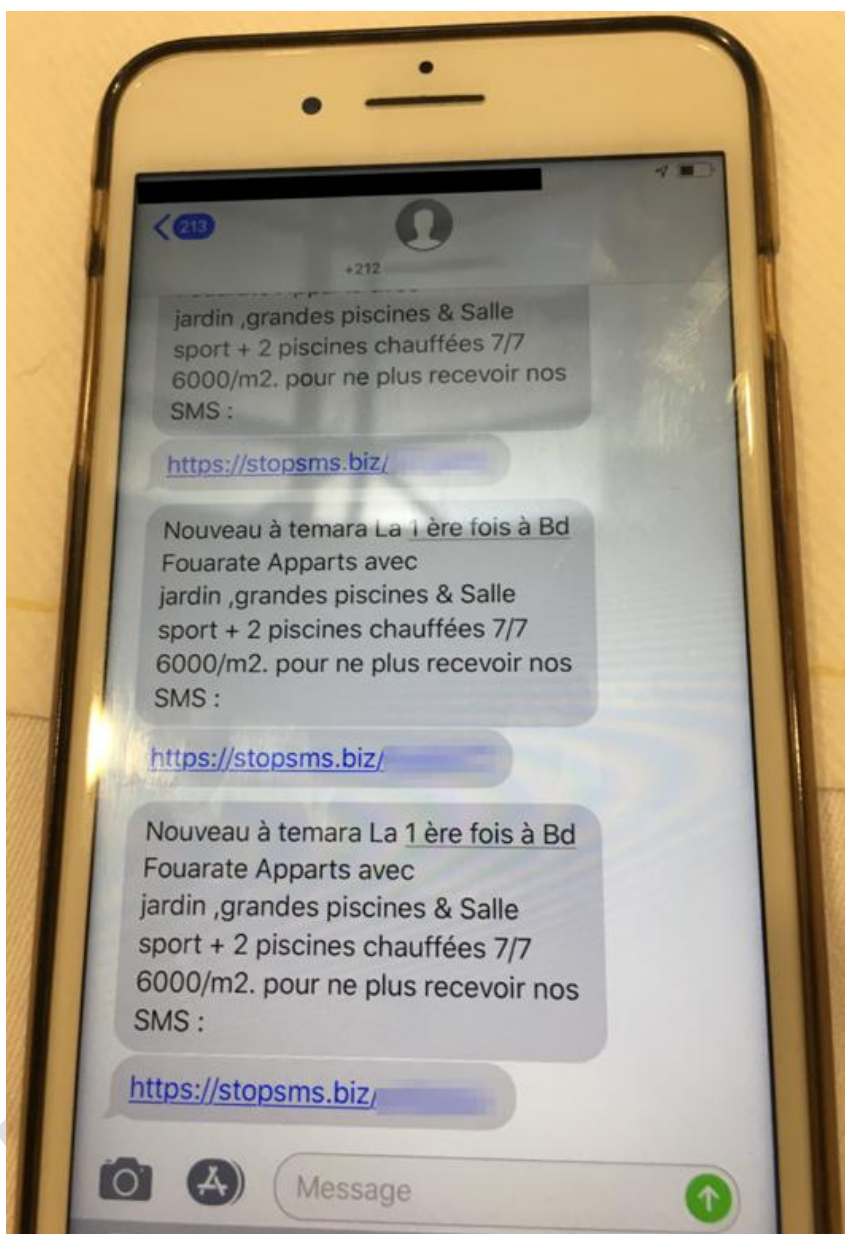
⁷² The full evidence used to attribute the DGST as the single Moroccan customer of Pegasus is detailed in Section 4.3.

⁷³ Independent, "Amnesty claims jailed Moroccan journalist was targeted by Rabat using Pegasus spyware before being arrested", 21 July 2021, <https://www.independent.co.uk/news/world/middle-east/morocco-pegasus-spyware-b1887455.html>

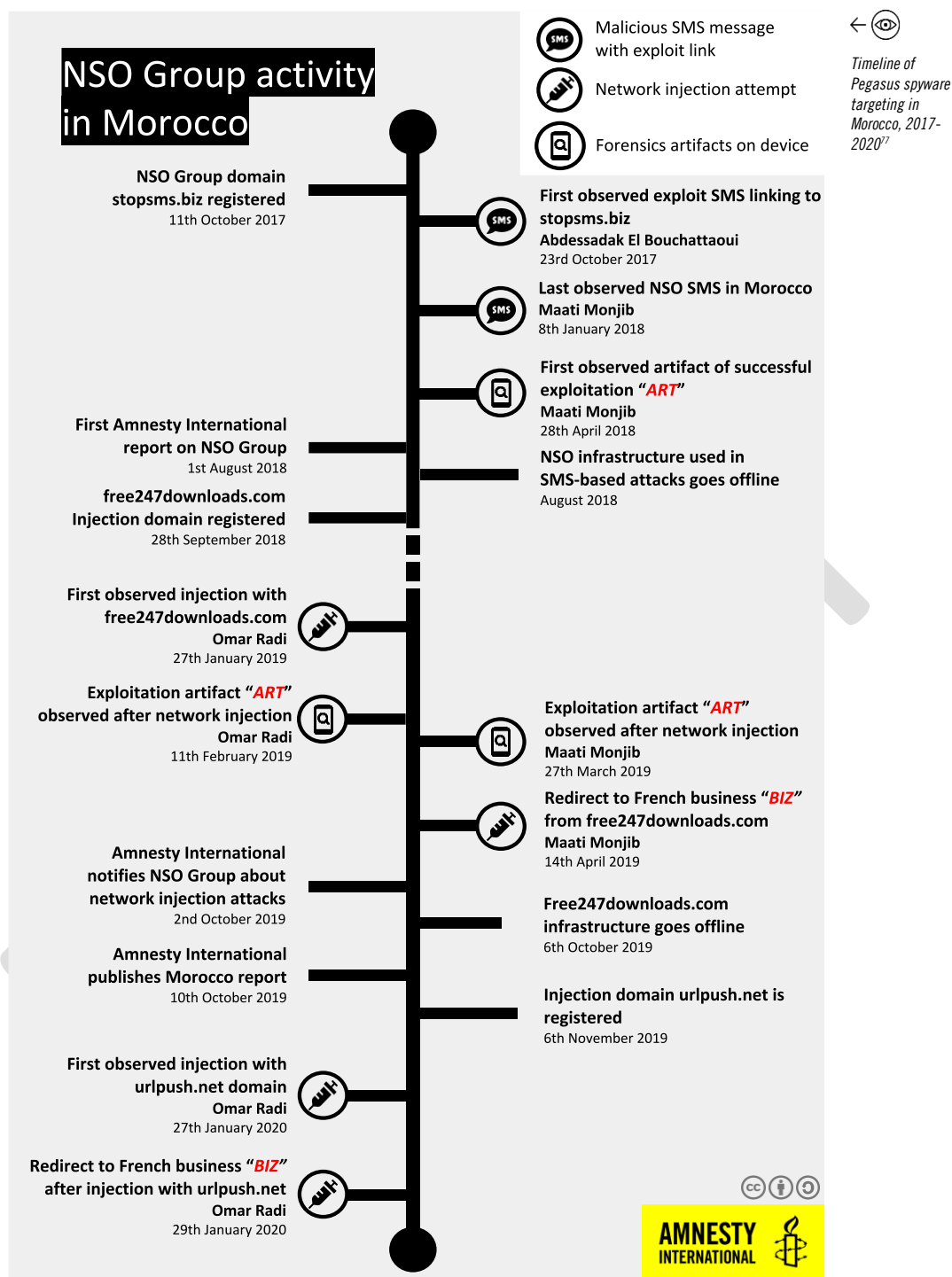
⁷⁴ Haaretz, "Israel issues stricter guidelines for cybertech exports after NSO scandal", 12 June 2021, <https://www.haaretz.com/israel-news/tech-news/2021-12-06/ty-article/israel-issues-stricter-guidelines-for-cybertech-exports-after-nso-scandal/0000017f-f2b3-df98-a5ff-f3bde340000>

⁷⁵ Haaretz, "Israel torpedoed Morocco spyware deal - and NSO competitor QuaDream shut down", 23 May 2023, <https://www.haaretz.com/israel-news/security-aviation/2023-05-23/ty-article/premium/israel-torpedoed-morocco-spyware-deal-and-nso-competitor-quadream-shut-down/00000188-425a-d805-a7c9-dbbdb7f50000>

⁷⁶ Amnesty International, "Hirak el Rif appeal must deliver justice after deeply flawed trial," 17 December 2018, <https://www.amnesty.org/en/latest/news/2018/12/morocco-hirak-el-rif-appeal-must-deliver-justice-after-deeply-flawed-trial-2/>

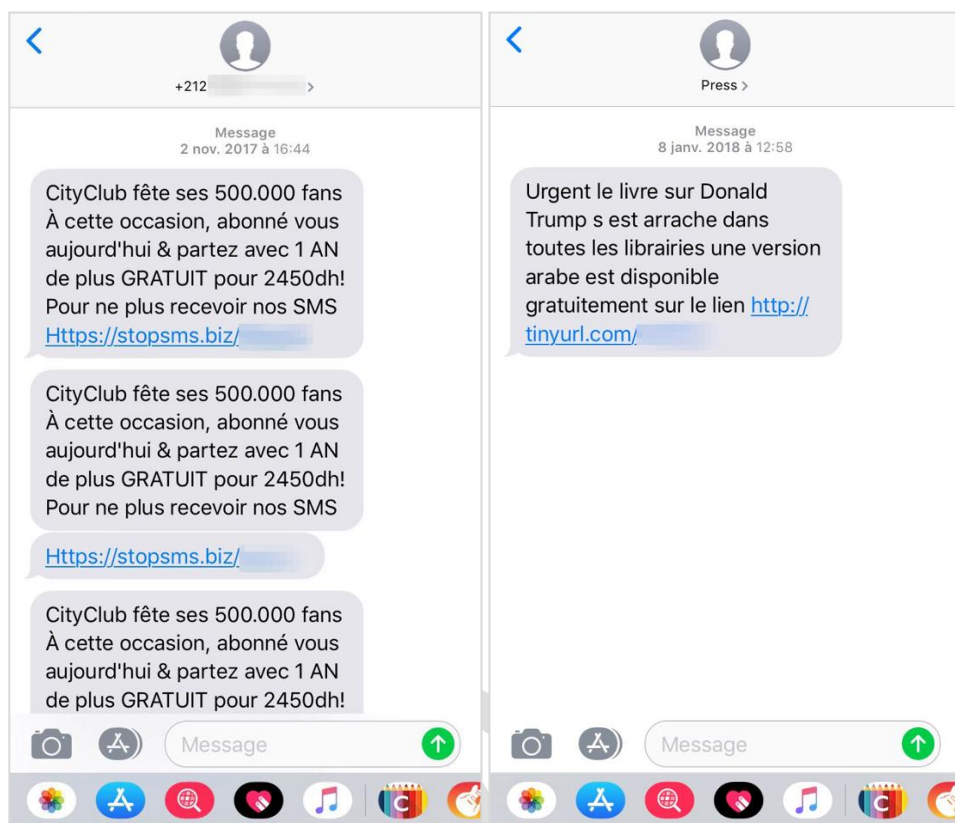


Multiple Pegasus
1-click infection links
sent to Abdessadak El
Bouchattaoui's mobile
phone in 2017



Similarly, the phone number of human rights defender Maâti Monjib was *selected* as a Pegasus target by the Moroccan Pegasus customer on 11 September 2017. Pegasus Project records show his number was *selected* for targeting again on multiple occasions over the following two years including on 2 November 2017 and 8 January 2018. On both of these days, the *selection* occurred shortly before he was sent the Pegasus 1-click infection SMS messages.

⁷⁷ Amnesty International, "NSO spyware used against Moroccan journalist", June 2020, <https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/>



Pegasus SMS messages sent to Maâti Monjib in November 2017 and January 2018

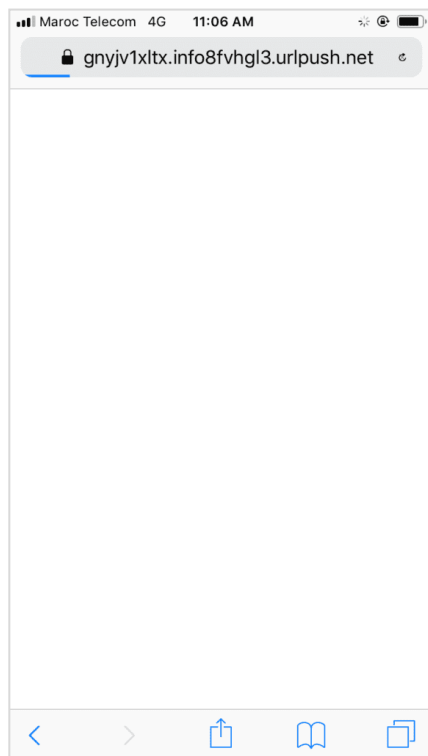
5.1.2 NETWORK INJECTION ATTACKS

Drawing on both technical research, including past documented cases, and source testimony from *Safir*, a former DGST intelligence official, Amnesty International can confirm that Moroccan authorities and the DGST also began using another powerful spyware infection technique from 2018 onwards: network injection. Network injection relies on the spyware operator being able to manipulate the internet traffic of a target in order to direct their browser to a malicious infection link.

Amnesty International's technical research found that such traffic manipulation in Morocco was carried out by means of a network injection system installed in the network of Maroc Telecom, the partially state-owned telecommunications company. Since NSO Group's technology is sold exclusively to government customers, and a network injection would require privileged access to Morocco's national mobile infrastructure, Amnesty International concluded that Moroccan authorities were responsible and that they were using Pegasus to target human rights defenders and journalists. This was later further substantiated by leaked NSO documents and testimony from *Safir*.

In 2020, Amnesty International identified network injection attacks being carried out through the Maroc Telecom network after the discovery of malicious redirects and Pegasus infection attempts on the phone of Moroccan journalist Omar Radi.⁷⁸ At the time of the malicious redirects, Omar Radi was connected directly to the Maroc Telecom network over 4G. The screenshot, and specifically the domain, prove that the network injection was being triggered by the mobile network rather than a malicious WiFi network or tactical network element.

⁷⁸ Amnesty International, "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools", 22 June 2020, <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/>



Screenshot of live network injection infection attempt against Omar Radi using Pegasus infection domain urlpush[.]net while connected to the Maroc Telecom 4G network⁷⁹

Interviews with *Safir*, a former DGST intelligence official, confirm the role of the DGST as the specific agency working with NSO Group and with Maroc Telecom to enable the network injection capability. *Safir* stated that Maroc Telecom permitted the installation of technology to facilitate network injection attacks, though this does not imply that they would have been aware of, or directly participated in attacks taking place. *Safir* also described how a telecommunications provider in Morocco also assisted in the spyware targeting process by providing device identifiers associated with target phone numbers such as the phone's IMEI. IMEI numbers allow a specific device on an operator's network to be identified, while also providing information on the make and model of the phone which can be used to determine suitable infection vectors.

Safir described the active involvement of a domestic telecommunications company in facilitating spyware operations. The company provided customer phone numbers to the DGST and other identifiers allowing for zero-click attacks as well as discreetly providing targets with unlimited data packages, so that the extraction of their data via Pegasus did not trigger their data caps and arouse suspicion.

In 2019, Amnesty International published the first ever forensic evidence confirming Pegasus spyware infection of the mobile phones of human rights defenders and activists, rather than just targeting attempts. The spyware targets featured in that research – human rights defender Maâti Monjib and lawyer Abdessadek El Bouchettaoui – were targeted by both 1-click infection links and suspected zero-click network injection attacks.⁸⁰ The network injection findings were later confirmed in 2020 when journalist Omar Radi's device was also infected with Pegasus while connected to the Maroc Telecom network.

5.1.3 ZERO-CLICK ATTACKS

Amnesty International observed evidence of Pegasus 1-click infection links being sent in Morocco from October 2017 until January 2018. From February 2018 onwards the first evidence of zero-click infections was found in Morocco, suggesting that around this time NSO Group provided their Moroccan customer (the DGST) with the capability to perform zero-click ("Covert") attacks against Moroccan Pegasus targets, expanding from 1-click attacks.

⁷⁹ Amnesty International, "NSO Group spyware used against Moroccan journalist days after company pledged to respect human rights", 22 June 2020, <https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/>

⁸⁰ Amnesty International, "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware" (previously cited); Amnesty International, "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools", (previously cited).

Infection traces which were consistent with Pegasus zero-click attack vectors, specifically those involving browser exploitation, were found on the device of Maâti Monjib from February 2018. In early 2018, NSO Group was in the process of rolling out their upgraded Pegasus 3 and a suite of new zero-click infection vectors.

Internal NSO Group material disclosed as part of the WhatsApp case provides more details about the zero-click infection vectors used in this time period. For Android devices, zero-click vectors targeting via WhatsApp were the only Covert/zero-click vector method in the 2018-2020 period, although the exact underlying exploit changed over this time (Heaven, Eden, ERISED).⁸¹ Heaven was first released for production use around April 2018,⁸² shortly before NSO Group representatives travelled to Morocco in May 2018 to train operators on the upgraded system.⁸³

NSO Group also had multiple iOS vectors during that time, although the WhatsApp material is less detailed on these vectors. A zero-click vector “Diablo” was available in 2018 and likely corresponds to an exploit targeting iOS 11.X devices observed forensically as targeting Voice-over-WiFi services.⁸⁴ NSO Group later rolled out a new iOS 12.X vector “Dragonfly” which targeted via iMessage. The vector was used very actively by Morocco throughout 2019 until the vector was likely inadvertently mitigated when Apple released the iOS 12.4.1 software update.⁸⁵ NSO Group and Morocco continued to use further iPhone zero-click exploits into 2021 including an iOS 13 vector targeting Apple Photos and multiple iMessage zero-click vectors.

Safir described the evolution of the Pegasus system in Morocco from 1-click to zero-click as new infection vectors became available:

“NSO’s vector attacks... had a lot of choices on the entry door. Especially on Android they had a lot of entry doors. They had exploits on the core service of Android. On iPhone they were using iMessage exploits since the end of 2017, same for the redirection to use the Webkit vulnerability. These are vector attacks. In 2017 we needed the user interaction, we needed them to click on links.”

Safir goes on to describe other vectors which could be used to exploit Android phones remotely based on vulnerabilities on the core telephony service on Android, which may refer to the targeting of Rich Communication Services (RCS) or another component of the Android telephony software:

“But in 2019 they showed us attacks using vulnerabilities on the system level in Android. They showed us one attack where they made an anonymous phone call and five seconds later the phone was infected. Android is filled with holes. The exploit was on the system level at the core telephony service of Android. The payload was sent through a call made via the gateway equipment that was installed in the infrastructure of [a telecommunications provider]. It was called ‘injection method via gateway...’. There were many methods, you can select attack through 2G or 4G. The infection servers were already installed in the telecom network which made it easier for attacks.”

Safir’s testimony also provides insight into what it was like for an operator to use Pegasus. He likened the Pegasus interface to a messaging app from the early 2000s: on the dashboard each target or “operation” has its own folder which corresponds to a user ID. The folder contains organized files related to that individual, ready to view with just a click. *Safir* said: “messages, calls, photos, it’s all there”.⁸⁶

5.1.4 MOROCCAN GOVERNMENT ABUSIVE USE OF PEGASUS TO TARGET HRDS

In 2019, seven Moroccan activists were notified that their phones were hacked via WhatsApp using Pegasus spyware.⁸⁷ In November that year, eight victims who received the same notification filed a complaint to Morocco’s National Control Commission for the Protection of Personal Data (CNDP).⁸⁸ At the time of publication in 2026, the complainants had not received a direct response from CNDP.

⁸¹ [Add excerpt from NSO engineer testimony describing the various Heaven vectors as the only zero-click vectors available on Android.]

⁸² [Add footnote to Heaven roll out doc]

⁸³ See Section 4.3 which describes trainings conducted by NSO Group for the Moroccan customer.

⁸⁴ [Add footnote for Diablo]

⁸⁵ Virus Bulletin, *Exploit archaeology: a forensic history of in-the-wild nso group exploits*, (previously cited).

⁸⁶ Interview with *Safir*

⁸⁷ Abdellatif el-Hamamouchi, “How Israeli Company NSO Hacked My Phone”, 25 November 2020, smex.org/how-israeli-company-nso-hacked-my-phone/

⁸⁸ Human Rights Watch, “They’ll Get You No Matter What”: Morocco’s Playbook to Crush Dissent (previously cited). <https://www.hrw.org/report/2022/07/28/theyll-get-you-no-matter-what/moroccos-playbook-crush-dissent>

In July 2021, Amnesty International confirmed the use of Pegasus zero-click attacks against many additional Moroccan journalists and human rights defenders. As part of the Pegasus Project, Amnesty International's Security Lab partnered with Forbidden Stories and a consortium of more than 80 journalists from 17 media organizations in 10 countries.⁸⁹

Amnesty International was able to directly confirm the presence of traces of Pegasus spyware through forensic analysis of several devices belonging to people whose numbers were on the list of targeted individuals uncovered in the Pegasus Project. Among them were journalist Hicham Mansouri (a Moroccan journalist who received asylum in France), activist Claude Mangin (wife of Sahrawi political prisoner Naâma Asfari), and Joseph Breham (a French human rights lawyer whose cases included Sahrawi activists in Morocco).

Activists from Western Sahara were also targeted. Oubi Bouchraya Bachir, a political activist and former representative of the Sahrawi liberation movement Polisario Front to the European Union,⁹⁰ and Aminatou Haider, a Sahrawi human rights defender, were also targeted with Pegasus. Amnesty International's Security Lab forensically confirmed traces of infection on Aminatou Haider's device in October and November 2021, months after the Pegasus Project revelations.⁹¹

Whistleblower testimony in this report on the use of Pegasus in Morocco is consistent with Amnesty International's own research findings, including the timeline of initial deployment and the identities of the initial civil society targets on whom Moroccan officials were spying within weeks of the installation of the system.

5.1.5 DENIAL AND BACKLASH FROM THE MOROCCAN AUTHORITIES

Despite detailed forensic findings of unlawful Pegasus surveillance by Morocco, and independent threat notifications by WhatsApp to prominent Moroccan civil society members about suspected Pegasus spyware targeting, the Moroccan authorities have consistently denied allegations that they have used spyware to target civil society.

Following Amnesty International's 2020 report on the Pegasus attacks against Omar Radi, Moroccan authorities denied the findings. They said they "categorically reject" what they described as "baseless allegations", adding that "publication of the report [...] is part of an agenda targeting Morocco".⁹²

The Moroccan government falsely accused Amnesty International of failing to offer them the right of reply on the findings of the report, and of fabricating facts and failing to provide evidence to back up the claims made within it. On the contrary, Amnesty International notified the Moroccan authorities on 9 June 2020 through an official letter sent via email to five officials at the Ministry of Human Rights, of its intention to publish the report two weeks prior to publication. The same letter invited the government to provide comment for inclusion in the report. However, no response was received.⁹³ A smear campaign was launched against Amnesty International in Moroccan media and social media.⁹⁴

On 23 July 2021, in response to Amnesty International's further findings as part of the Pegasus Project, Morocco filed a lawsuit before the Criminal Court in Paris against Amnesty International France and Forbidden Stories, citing defamation. The Court ruled that the complaint was inadmissible. Morocco appealed the decision and, in April 2023, the Court of Appeals upheld the lower court's decision. In response, Morocco filed an appeal with the Court of Cassation but withdrew its appeal in October 2023. In 2021, the Moroccan authorities also filed complaints in Germany against the German media outlets Die Zeit

⁸⁹ Forbidden Stories, "The Pegasus project: A worldwide collaboration to counter a global crime", 18 July 2021, <https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/>

⁹⁰ Yabiladi News, "Polisario reshuffles leadership Oubi Bachir Bouchrya reassigned from Geneva to Tindouf", 10 July 2025, <https://en.yabiladi.com/articles/details/171306/polisario-reshuffles-leadership-oubi-bachir.html>

⁹¹ Amnesty International, "Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence" (previously cited).

⁹² See: Morocco World News, Morocco 'Rejects' Amnesty International's Allegations of Cyber Spying, June 2020, <https://www.moroccoworldnews.com/2020/06/68551/morocco-rejects-amnesty-international-recent-allegations-cyber-spying/> and Arab News Japan https://www.arabnews.jp/en/middle-east/article_20318/ See: Morocco World News, Morocco 'Rejects' Amnesty International's Allegations of Cyber Spying, June 2020, <https://www.moroccoworldnews.com/2020/06/68551/morocco-rejects-amnesty-international-recent-allegations-cyber-spying/> and Arab News Japan, Moroccan authorities deny using spyware to monitor critics, June 2020,

⁹³ Amnesty International wrote to the Moroccan authorities in 2020, outlining evidence on the use of Pegasus spyware against Maâti Monjib, Abdessadek El Bouchettaoui and Omar Radi, and with recommendations for reforms of the regulatory framework that governs surveillance. Amnesty International did not receive a response to the letter. Amnesty International, English translation of letter sent in Arabic to Chief of Government of the Kingdom of Morocco (previously cited).

⁹⁴ Amnesty International, "Morocco and Western Sahara: Government smear campaign against Amnesty International underlines intolerance of scrutiny", 4 July 2020, <https://www.amnesty.org/en/latest/news/2020/07/morocco-and-western-sahara-government-smear-campaign-against-amnesty-international-underlines-intolerance-of-scrutiny/>

and Süddeutsche Zeitung, but these were rejected by Germany's Federal Court of Justice on 24 February 2026.⁹⁵

5.2 MORGAN: MOROCCO'S PEGASUS OPERATOR REVEALED

Based on an extensive analysis of the legal filings in WhatsApp and Meta's case against NSO Group, leaked surveillance records, open-source intelligence and first-hand whistleblower testimony, Amnesty International identifies with high confidence that Morocco's DGST is the end-user responsible for the use of Pegasus against Moroccan and Sahrawi civil society and for surveillance operations outside of Morocco and Western Sahara.

In 2025, as part of the *WhatsApp v. NSO* court case in the USA, a significant number of depositions, documents and internal NSO material were unsealed and made public by the court. One particularly informative document is a redacted and partial version of a presentation given to the board of Q Cyber Technologies, NSO Group's parent company, on 1-2 August 2018. The presentation provides a status update on the key developments with Q Cyber customers in the second quarter of 2018. Pegasus customer code names mentioned included Apollo, Subaru (identified by Haaretz as Saudi Arabia), Rolls-Royce, Aziza, Tinkerbell, Shemer and Morgan. According to reporting by Haaretz, NSO Group customers are given code names based on the first letter of the country's name and an automotive manufacturer.⁹⁶

CS Q2 Main Client Efforts

- 2 new clients added: Rolls-Royce and Aziza
- 1 Clients resume to service – Tinkerbell
- Heaven has been deployed at 10 clients
- Nighthawk has been deployed at 1 client – Maira 4 (beta)
- PGS 3 Beta has been deployed at 2 clients: Shemer, Morgan and 1 production client: Aziza.
- 16 trainings have been conducted to 12 clients. 5 PGS and 11 SE
- Storm - POC for 2 client (Oz and Raven)

80

Confidential & Proprietary © Q Cyber Technologies and its affiliates. All rights reserved.



Pegasus presentation

The presentation indicates that “Pegasus 3 Beta” was deployed to the customer code-named “Morgan” at some point before the board meeting in August 2018. Based on NSO's known name schema, which uses code names with the same first letter as the customer country, the exclusion of other known Pegasus customers beginning with M,⁹⁷ and the matching timeline, it can be inferred that “Morgan” was NSO Group's code name for their Moroccan customer, sharing three initial letters. As part of the *Pegasus Project*:

⁹⁵ Federal Court of Justice, <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2026/2026036.html> (accessed on 4 August 2026).

⁹⁷ Specifically, Mexico and Malaysia. Mexico's multiple customers are code-named “Mercedes” and potentially as also “Maira”. Malaysia is referred to as “Mazda”.

Inside Morocco's Spying Machine investigation, Forbidden Stories reported that "several sources within the cyber-surveillance industry have confirmed that Morocco's codename at NSO is "Morgan."⁹⁸

5.2.1 EARLY PEGASUS CUSTOMER TESTING EXPOSES THE SPYWARE OPERATORS

From September 2017 onwards, the DGST deployed and used Pegasus. NSO Group staff conducted demonstrations of the system for the DGST following the initial deployment and each time they rolled out new versions and functionalities.

The Pegasus Project records show that in late June and early July 2017, four unique Moroccan phone numbers were selected as Pegasus spyware targets, apparently as part of a Pegasus sales demonstration rather than any real customer use of the Pegasus system. Material released as part of a civil action by WhatsApp against NSO Group shows that such systems were used by NSO Group sales staff and pre-sales engineers to perform live infections against test devices to demonstrate the capabilities of the product (see Section 4.1.3).

In late August 2017, new Pegasus activity was taking place in Morocco. Over the following month, Pegasus Project records and publicly available OSINT data show the Pegasus system being set up and initial targets being configured in the system. The full installation, testing and launch of a Pegasus system can take up to 16 weeks, according to leaked Pegasus system documentation. The real target phone numbers being entered in the system alongside apparent tests from DGST staff members indicates operators testing and setting up targets in the system in real time. In many cases, there are just minutes between a target being entered into the system and further test entries from DGST staff operating the system.

Technical records from the Pegasus Project show that several Moroccan phone numbers were entered into the Pegasus system during September 2017, including some numbers used for the earlier July demo. Intermittent with these test numbers, Amnesty International was able to identify and directly attribute some of these phone numbers to named individuals working at the DGST, based on open-source intelligence.

Table 1: DGST staff members phone numbers entered in Pegasus system during deployment.

PHONE NUMBER	OWNER	FIRST SEEN (UTC)	LAST SEEN (UTC)
+212*****499	DGST Agent B	2017-09-10 13:50	2018-05-01 13:31
+212*****517	DGST Agent B	2017-09-10 14:08	2019-02-08 09:41
+212*****318	DGST Agent A	2017-09-10 14:32	2019-05-26 14:27

Among those was a phone number for *DGST Agent A*, the person named by *Safir* as the head of the department with the DGST that was in charge of digital surveillance. A search in the ViewCaller caller ID service returned a result that matched the first name of this individual. The phone number associated with *DGST Agent A* was entered into the Pegasus system on 10 September 2017, before the system became operational. Amnesty International was also able to find a public document listing *DGST Agent A* as a representative of the DGST.

On the same date, two phone numbers associated with another DGST staff member, *DGST Agent B*, were also entered into the system for the first time, apparently also for testing purposes. OSINT services and phone caller ID databases were used to identify *DGST Agent B* as the owner of both phone numbers. One of his numbers was displayed by the ViewCaller service suggesting that *DGST Agent B* has a technical or engineering role in the DGST. Similar records created during system testing were found during investigations into other Pegasus customers, and it appears to have been a common practice as part of system testing.⁹⁹

⁹⁸ See Guardian, "Moroccan intelligence insider reveals widespread use of Pegasus hacking software", 16 July 2026, <https://www.theguardian.com/news/2026/jul/16/morocco-intelligence-insider-reveals-widespread-use-hacking-software-pegasus> and Forbidden Stories, "Codename "Morgan": how Morocco accessed Pegasus, involving Israel and the United Arab Emirates", 16 July 2026, <https://forbiddenstories.org/codename-morgan-a-look-back-at-moroccos-acquisition-of-pegasus-involving-israel-and-the-united-arab-emirates/>

⁹⁹ Direkt36, "Hungarian intel officer involved in spyware operations appears on Pegasus list", 29 October 2021, <https://www.direkt36.hu/en/kemsoftverekkel-is-foglalkozo-magyar-titkosszolga-kerult-elo-a-pegasus-listabol/>

Both *DGST Agent A* and *DGST Agent B* have previously been linked to Moroccan cyber-surveillance procurement. Their names were mentioned in an email included in 2015 leaked “Hacking Team” (Italian cyber-intelligence company) documents in relation to planned attendance at a surveillance technology fair (see Section 6.1 below for more analysis of Hacking Team’s products and their use in Morocco). Phone numbers for both individuals continued to be entered in the Moroccan Pegasus system during 2019, suggesting an ongoing role in the targeted surveillance operations and human rights violations tied to Pegasus.

Amnesty International cross-referenced the numbers in the Pegasus Project records associated with the DGST, the Moroccan customer, to validate these claims. Eight phone numbers linked to at least five suspected DGST officers named by *Safir* or identified through open-source research were found to be present in the Pegasus Project leak. Notably, two of these individuals – with previous links to the deployment of mercenary spyware – were seen most frequently in the data during the first month that the system was deployed in September 2017. *Safir* indicated that the system was first installed in September 2017, and indeed this is when targeting records tied to the Morocco customer first appear in the Pegasus Project leak.

These early targeting records were likely created as DGST staff members and engineers were testing the Pegasus system before it was made fully operational. Similar evidence was found in the Pegasus Project for other countries, including Hungary, where an operator responsible for technical surveillance had entered his own phone numbers into the Pegasus dashboard, likely to test the system.¹⁰⁰

Safir also identified a separate DGST officer who had volunteered their phone for a Pegasus on-site demonstration by NSO Group staff in 2018. *Safir* provided a phone number belonging to this individual, which Amnesty International could confirm – based on Pegasus Project records – was entered into the Morocco Pegasus system in May 2018. Amnesty International also identified an additional phone number tied to the same DGST officer entered in the system on the same day. These findings corroborate *Safir*’s first-hand knowledge on the demonstrations carried out by NSO and the deployment of the Pegasus spyware by the DGST.

As outlined in the previous chapter, in addition to deployed Pegasus customer systems, NSO Group maintained standalone Pegasus systems used to test features and to perform product demonstrations for potential or existing clients. Between 17 December and 19 December 2018, two Moroccan phone numbers were entered repeatedly into one of these separate NSO Group-controlled sales demo Pegasus systems.

This followed WhatsApp implementing a server-side block for the initial Heaven WhatsApp vector on 5 December 2018. This suggests that NSO Group was actively testing functionality or demonstrating new Pegasus features at this time. The same demo numbers were later selected in the Morocco customer system on 24 December 2018 and 17 January 2019.

5.3 HUMAN RIGHTS DEFENDERS AMONG THE FIRST TARGETS

Between 10 and 11 September 2017, the first real phone numbers of later confirmed Pegasus targets began to be entered in this system. The system was not yet active at this time, so these entries likely reflect cases and operations being set up in the system, potentially as part of further testing. In the first two days, the phone numbers were entered for prominent human rights defenders and independent journalists as the first intended targets (see **Table 2**). These include the phone numbers of journalists Taoufik Bouachrine (see case study of Afaf Bernani in Chapter 8) and Ali Anouzla, alongside human rights defenders Ahmed Benseddik, Maâti Monjib (case study in Chapter 7), and Fouad Abdelmoumni (case study in Chapter 7).

Table 2: Excerpt from Pegasus Project records showing phone numbers selected by Moroccan customer on 10 – 11 September

TARGET PHONE NUMBER	NAME ASSOCIATED WITH PHONE NUMBER	DATE ENTERED
+212*****	Taoufik Bouachrine	2017-09-10 13:22
+212*****499	<i>DGST Agent B</i>	2017-09-10 13:50

¹⁰⁰ Direkt36, “Hungarian intel officer involved in spyware operations appears on Pegasus list” (previously cited).

TARGET PHONE NUMBER	NAME ASSOCIATED WITH PHONE NUMBER	DATE ENTERED
+212*****499	DGST Agent B	2017-09-10 13:52
+212*****517	DGST Agent B	2017-09-10 14:08
+212*****318	DGST Agent A	2017-09-10 14:32
+212*****499	DGST Agent B	2017-09-10 14:35
+212*****	Taoufik Bouachrine	2017-09-11 09:01
+212*****	Ahmed Benseddik	2017-09-11 11:19
+212*****	Ali Anouzla	2017-09-11 11:21
+212*****	Maâti Monjib	2017-09-11 11:22
+212*****499	DGST Agent B	2017-09-11 11:24
+212*****	Taoufik Bouachrine	2017-09-11 11:28
+212*****499	DGST Agent B	2017-09-11 11:33
+212*****	Fouad Abdelmoumni	2017-09-11 11:37
+212*****517	DGST Agent B	2017-09-11 12:58
+212*****	Taoufik Bouachrine	2017-09-11 13:08

An analysis of all target phone numbers entered in the Moroccan Pegasus system between September and December 2017 provides further evidence that human rights defenders were the priority targets of the DGST. Excluding testing and internal phone numbers, Amnesty International was able to match 103 Moroccan phone numbers with specific named individuals. Of those people selected as potential Pegasus targets, 65 were identifiable as civil society members (including 34 human rights defenders, 22 journalists and media worker, 5 lawyers, and 4 academics), 25 were political representatives or officials, 5 were diplomats or representatives of international organizations. The remaining 8 identified individuals include business people, religious figures and others whose identity or categorisation was unclear.

These records show the phone numbers of prominent human rights defenders and journalists were among the first to be entered into the Pegasus system, indicating that this was the priority purpose for which the DGST had acquired the highly invasive spyware system. The focus on civil society members was a core purpose, rather than incidental.

5.3.1 ADDITIONAL NSO-CONNECTED SYSTEM DEPLOYED IN MOROCCO AT THE SAME TIME AS PEGASUS SYSTEM DEPLOYMENT

Amnesty International assesses with high confidence that a Moroccan VPN server linked with Circles is also tied to Morocco's deployment of Pegasus, either as part of a unified product or sold together with a Circles system, based on the analysis provided in this section.

Circles is a Bulgaria-based digital surveillance company affiliated with the NSO Group, established in 2008 to develop SS7-based location tracking technologies. It was acquired in 2014 by Francisco Partners and integrated into NSO Group.¹⁰¹ In a letter to Amnesty International in 2021, NSO Group indicated that the Bulgarian companies which are part of NSO Group "provide, on a contract basis, research and development services to their respective Cypriot affiliates and export the network products for governmental use".¹⁰²

¹⁰¹ Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure* (Index Number: DOC 10/4182/2021), 31 May 2021, <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>

¹⁰² Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure* (previously cited).

A 2018 board meeting presentation from Q Cyber Technologies SARL, a Luxembourg-based company affiliated with NSO Group (see the ‘Summary of companies and surveillance technologies’ table, above), and other material disclosed as part of the WhatsApp lawsuit, show that the companies Q Cyber Technologies and Circles were increasingly integrated by 2018, sharing the customer code names in some instances.¹⁰³ The board meeting overview noted that Q Cyber Technologies’ “Network & Tactical” products were located in Bulgaria.

In 2020, the Citizen Lab published a report documenting the proliferation of Circles’ technology.¹⁰⁴ Among the set of suspected Circles systems documented by Citizen Lab was a VPN server located on an IP address range 105.145.40.27-29, which Citizen Lab attributed to the Moroccan Ministry of Interior (see report excerpt below).

Morocco

Our scanning identified what appeared to be a single Circles system in Morocco. The Morocco client’s IPs are in the same /27 as several websites of the Bureau central d’investigation judiciaire (BCIJ), and are in the same /26 as the website of the Moroccan Auxiliary Forces (FA). Both the FA and BCIJ are under the auspices of Morocco’s Ministry of Interior. A government agency in Morocco also appears to be a client of Circles’ affiliate NSO Group, though the identity of this Moroccan agency has not been established.



Excerpt from Citizen Lab report on Circles deployment in Morocco¹⁰⁵

Client Name	Possible Identity	Seen in Scan	Firewall IPs
	Ministry of Interior	2018/3/14 – Present	105.145.40.27-28

TABLE 5

Citizen Lab’s scanning methodology found that the Moroccan VPN server was active and matching a suspected Circles VPN fingerprint from at least 14 March 2018 until early 2021.

Further analysis by Amnesty International’s Security Lab has found that the Moroccan VPN system was first deployed and visible on a Moroccan IP range as early as September 2017, the same month that the Moroccan Pegasus system also became active.

The Moroccan IP address range 105.145.40.27-29 hosted a VPN server with a self-signed certificate (with name “localhost”) from 12 September 2017 until 9 March 2021. The same certificate was also visible on a set of Bulgarian IP addresses linked to NSO Group. The Bulgarian IPs also hosted TLS certificates with the internal component “tracksystem[.]info” which had previously been used by NSO Group company Circles.

The VPN certificate was visible in Bulgaria for one day in August 2017 before later reappearing in Morocco. This suggests a VPN server or system that was first configured by NSO Group staff in Bulgaria before being shipped to the customer in Morocco (see annex 12.1 for tables of VPN server certificates visible in Bulgaria and then later in Morocco).

Notably, other certificates hosted on the same Bulgarian IP range associated with NSO Group closely correlate with other known Pegasus system deployments rather than Circles SS7 product deployments. The observed VPN certificates also do not explicitly mention Circles or refer to the customer as a Circles customer.

Analysis of other certificates found on the Q Cyber/NSO Group linked IP 84.1.246.230 helps support the connection between these VPN servers and Pegasus customer deployments (see Annex 12.1).

¹⁰³ One document refers to a Pegasus sales demo being performed in 2019 for customer “Porsche”. The demo was performed on Peruvian phone numbers, indicating the customer country is Peru. The Circles system identified by Citizen Lab in Peru was code-named “Porsche Pisco”, showing NSO and Circles used a common naming system for customers.

¹⁰⁴ Citizen Lab, *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*, 1 December 2020, <https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>

¹⁰⁵ Citizen Lab, *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles* (previously cited), section ‘Morocco’.

An earlier certificate – “client-dutton-dolce VPN Certificate” – also appears to be tied to a Pegasus deployment. In testimony released as part of the WhatsApp case, an NSO group representative identified “DUTTON” as their customer code name for the Emirate of Dubai.¹⁰⁶

The observed timeline for the VPN certificate creation and scanning for the confirmed DUTTON customer matches closely with the timeline of the Dubai Pegasus system deployment and operation. This suggests that these VPN certificates may indeed represent Pegasus system deployments rather than a separate Circles product deployment.

Pegasus Project records for the Dubai/DUTTON customer show that first Pegasus testing activity began on 27 October 2016, the same day the VPN certificate was issued. The testing activity continued over the following month. The first identifiable Pegasus target was entered in the system on 7 December 2016, two days after the VPN certificate was seen active on the Dubai IP address ranges.

The findings for the certificate and customer linked to Morocco are similar. The first Moroccan numbers were seen in tests in July 2017. The Moroccan customer system was under testing from the start of September 2017. The first identifiable Pegasus targets were entered in the system on 9 September 2017, three days before the VPN certificate was first seen in Morocco on the IP range associated with the Ministry of Interior and the DGST.

Amnesty International assesses with high confidence that the VPN system installed on the Moroccan Ministry of Interior IP range in September 2017 is tied not just to Circles but also to NSO Group and Q Cyber Technologies, companies to which it is affiliated. The evidence further suggests that the TLS certificates are related to Moroccan Pegasus customer deployment.

Amnesty International has reviewed leaked Moroccan intelligence files that show the domain name “tersim.ma” is an email domain used internally by the DGST. The email server for this domain is hosted at 105.145.40.3 in the same /27 IP range as the NSO Group-linked VPN server. The same email server also handles the domain “bcij.gov.ma” for the Bureau central d’investigations judiciaires (BCIJ), a judicial police service that works closely with the DGST, affiliated with “mis.gov”. The same email address used to register “tersim.ma”, “bcij.gov.ma” and “mis.ma” was also used to register the domains “dgst.gov.ma” and “dgst.ma”, further linking the IP range to the Moroccan DGST.¹⁰⁷

5.4 MOROCCO’S USE OF PEGASUS SPYWARE BEYOND ITS BORDERS

This section examines how Morocco expanded its use of Pegasus outside its borders to target Moroccan activists and journalists, lawyers, military officials, diplomats, and senior political leaders across Europe, with a particular focus on France and Spain.

This analysis is based on three independent but mutually reinforcing sources of evidence. Firstly, it draws on detailed Pegasus Project records spanning the time frame from when Morocco first obtained Pegasus to mid-2019, which includes thousands of phone numbers entered in the Moroccan Pegasus system for potential targeting. Not all numbers entered in the system (termed here as “*selected*”) will ultimately have received a Pegasus infection attempt or have been successfully infected. Only forensic analysis on targeted devices can be used to confirm without doubt that a phone number *selected* for targeting with Pegasus was infected.

Secondly, this section draws on forensic investigations carried out by Amnesty International on the devices of individuals in Europe which Pegasus Project records show were *selected* by Morocco. On many of the analysed devices, evidence of successful Pegasus spyware targeting and infection was found, often shortly after the target phone numbers were *selected* on the customer side. The repeated temporal correlation between target selection and forensically confirmed infections confirms that Morocco was actively targeting and successfully infecting the phones of individuals outside the country, as suggested by the Pegasus Project data.

Thirdly, because NSO Group creates unique attack infrastructure (domain names, servers and email addresses) for each customer, it is possible to use specific attack infrastructure - such as attacker iCloud accounts – to link (or *cluster*) multiple Pegasus infections as having been performed by the same Pegasus

¹⁰⁶ District Court, N.D. California, WhatsApp Inc. v. NSO Group Technologies Limited, Case 4:19-cv-07123, Document 796-2, , pp. 8-16. storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.796.2.pdf

¹⁰⁷ tersim2019@gmail.com

customer. Different indicators can also be linked together based on their co-occurrence on the same targeted devices. These clusters of forensically observed indicators can then be conclusively attributed back to a customer, in this case Morocco – based on the close correlation with Morocco’s target selection (as seen in the Pegasus Project data and victim profiles from the cluster, including Moroccan journalists alongside human rights lawyers, and politicians).

Taken together, this evidence reveals the broad set of individuals *selected* as targets by Morocco. The forensic analysis confirms that the selections led to Pegasus infections, and the account attribution shows that a single Moroccan system controlled by the DGST was responsible for all of the targeting, from activists to government officials.

5.4.1 TIMELINE OF MOROCCO’S SELECTION OF PEGASUS TARGETS ABROAD

The first evidence that Morocco’s use of Pegasus spyware was expanding to targets outside the country began on 22 April 2018, when the first non-Moroccan phone number appeared in the Pegasus Project leak. The section draws on an analysis of the Pegasus Project dataset and identification of associated phone numbers. The logs show that the first Algerian phone number was associated with a prominent Sahrawi diplomat with the United Nations Mission for the Referendum in Western Sahara (MINURSO). The other numbers *selected* that day appear to have been largely Algerian military officials.

The following day, 23 April 2018, the logs show the first French numbers beginning to be *selected* in the system, beginning with exiled Moroccan journalist Aboubakr Jamaï. He was *selected* for Pegasus targeting extensively by Morocco over the following two years. On 1 May 2018, a French phone number for a Moroccan newspaper publisher (Jamal Boudouma) was first selected in the Pegasus system. Also on 1 May 2018, phone numbers for multiple DGST Pegasus operators, including *DGST Agent A* and *DGST Agent B* were again entered in the system. On 3 May 2018, a phone number for *DGST Agent B* was entered again and two phone numbers for another DGST staff member (*DGST Agent C*) were also entered on the system, likely while testing new functionality provided by NSO Group (see Section 4.2).

The selection of Algerian and French phone numbers continued extensively over the following weeks. Many of these phone numbers were only *selected* once. This could indicate that DGST operatives were entering potential targets broadly to check if they were vulnerable to zero-click attacks such as those for WhatsApp, which could be used reliably to infect targets outside the country. This WhatsApp exploit was only effective against Android users with a supported version of Android installed.

On 8 May 2018, the French phone number of a French human rights lawyer representing journalist Taoufik Bouachrine was *selected* as a target. Later the same day, a phone number for human rights defender and former prisoner Adil Lamtalsi was *selected*. Supported by ACAT-France, a French anti-torture NGO, Mr Lamtalsi had filed a complaint of torture at Paris High Court, alleging he was physically abused while held at the Temara secret detention centre, managed by the DGST.¹⁰⁸ The ACAT also documented allegations of torture made by Naâma Asfari, a Saharawi of Moroccan nationality, against officers of the DGST and others.¹⁰⁹ Joseph Breham, the human rights lawyer who represented Naâma Asfari in a complaint in respect of Morocco filed with the UN Committee against Torture, was also later *selected* as a target. Amnesty International later confirmed he was compromised with Pegasus on multiple occasions.

In reaction to these court filings, and an attempt by the French judicial police to question DGST Director General Abdellatif Hammouchi while he was present in France, the Moroccan authorities took the step to suspend judicial cooperation agreements with France.¹¹⁰ Morocco also filed a complaint in France against ACAT, Adil Lamtalsi and Naâma Asfari for defamation.¹¹¹

The first Spanish number *selected* by the DGST was on 11 May 2018, a phone number associated with Saharawi human rights defender Aminatou Haidar, who Amnesty International later forensically confirmed was infected by Morocco with Pegasus (see Case Study Saharawi activists, below).¹¹²

¹⁰⁸ ACAT, L’ACAT au cœur de la crise diplomatique franco-marocaine [“ACAT at the heart of the Franco-Moroccan diplomatic crisis”], 30 June 2014, acatfrance.fr/lacat-au-coeur-de-la-crise-diplomatique-franco-marocaine (in French).

¹⁰⁹ OHCHR, *Ennaâma Asfari v. Morocco*, Case 606/2014, 15 November 2026, <https://juris.ohchr.org/casedetails/2621/en-US>

¹¹⁰ BBC, “Morocco-France row over Hammouchi torture claims”, 26 February 2014, <https://www.bbc.co.uk/news/world-europe-26360224>

¹¹¹ Amnesty International, *Shadow of impunity: Torture in Morocco and Western Sahara* (Index Number: MDE 29/001/2015), 19 May 2015 <https://www.amnesty.org/en/documents/mde29/001/2015/en/>

¹¹² Amnesty International, “Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence” (previously cited).

After a slower period of targeting into the end of 2018, the targeting of Spanish and European numbers begins in a focused manner again from February 2019. Internal NSO Group communications, released as part of the civil case between WhatsApp and NSO Group, indicate that NSO Group had succeeded in developing their new Eden zero-click vector against WhatsApp on Android by 4 February 2019. Phone numbers of DGST Pegasus operators *DGST Agent A* and *DGST Agent B* were selected multiple times on 8 February 2019, around the same time these new vectors were becoming available.

On 25 February, the number of a Spanish activist leading an association supporting Saharawi independence was *selected* as a target. On 5 March, a Moroccan journalist based in Spain was targeted, Hussein Majdoubi. The same day Spanish journalist Ignacio Cembrero had his phone *selected* for targeting, reappearing 25 times over the following two months.¹¹³ Also on the same day, 5 March 2019, a Spanish phone number for Moroccan journalist Aboubakr Jamaï was *selected*. He had previously been first *selected* for targeting on his French phone number in 2018. Aboubakr Jamaï was later notified by WhatsApp that he had been targeted with Pegasus via a WhatsApp zero-click exploit in late April and early May 2019.¹¹⁴ Pegasus Project records show the DGST repeatedly *selected* Aboubakr's number for targeting on multiple days between 25 April and 10 May 2019, confirming that the notification he received from WhatsApp was as a result of Pegasus targeting carried out by the DGST. In a court filing, WhatsApp identified 69 Moroccan, 39 Algerian, 21 Spanish and 7 French phone numbers targeted during this same period.¹¹⁵ The WhatsApp filings do not identify the customer responsible, but it is likely that the majority of these 136 phone numbers were targeted by Morocco. Among the Spanish targets notified by WhatsApp were individuals later confirmed to have been targeted by a Spanish Pegasus customer.

On 6 March 2019 – the day after Aboubakr Jamaï's Spanish number was *selected* – the phone number for another DGST staff member, *DGST Agent C*, was entered again. Another phone number associated with him was *selected* again on 21 March and 19 April 2019, likely related to further training or testing activity. During this time period the DGST continued to heavily target Algerian phone numbers and phone numbers in France belonging to Moroccan civil society, journalists, French political figures and Algerian officials and diplomats. On 23 February 2019, Mediapart journalist Léniaïg Bredoux was *selected* for targeting by the Moroccan operator as evidenced by the Moroccan Pegasus Project records. Amnesty International later forensically confirmed that she was successfully compromised with Pegasus by the DGST on multiple occasions in 2019 and 2020.

On 13 March 2019, a French phone number associated with a former senior Algerian UN Special Envoy, Lakhdar Brahimi, was *selected*. One minute later a phone number of French President Emmanuel Macron was also *selected*.¹¹⁶ Three days later on 16 March, the phone numbers of Lakhdar Brahimi, French politician Leïla Aïchi, Belgian MEP Louis Michel and Emmanuel Macron were *selected* within 30 minutes of one another. Numerous other senior diplomats around the world were selected by Moroccan security officials in the same days. Later the same day, a Spanish phone number for Moroccan journalist Ali Lmrabet was first selected, and the French phone number for Aboubakr Jamaï was targeted again.

This extensive targeting of French numbers continued up until August 2019 when the Pegasus Project data related to Morocco ended, although Morocco continued to remain a Pegasus customer. A number of those French targets were later forensically confirmed as infected with Pegasus by Morocco including Claude Mangin, wife of jailed Saharawi activist Naâma Asfari, and Joseph Breham, a lawyer who represented Mr Asfari in his complaint filed against Morocco with the UN Committee against Torture.

This period of intense international targeting coincides with NSO Group's release of a powerful and reliable iOS zero-click vector which targeted iMessage. Forensic evidence shows that in many of the cases forensically analysed, selected phones showed signs of successful infection just minutes after being selected as targeted in the Moroccan Pegasus system.

¹¹³ Ignacio Cembrero is a journalist and media partner in this investigation.

¹¹⁴ Insert footnote about Aboubakr Jamaï's notification by WhatsApp

¹¹⁵ District Court, N.D. California, *WhatsApp Inc. v. NSO Group Technologies Limited*, Case 4:19-cv-07123, <https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.679.6.pdf>, p. 127.

¹¹⁶ President Macron was one of 14 heads of state whose phone number appeared in the leaked list of 50,000 potential surveillance targets revealed in the Pegasus Project in 2021. Amnesty International, "Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware", 20 July 2021, <https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/>

5.5 FORENSIC ATTRIBUTION OF ATTACKS TO MOROCCO BASED ON REUSED ZERO-CLICK ATTACK EMAIL ADDRESSES

The Pegasus Project records themselves provide clear insights into the targeting priorities and activity of the Moroccan Pegasus customer. This evidence of targeting by the DGST can be further validated with material evidence gathered through forensic analysis of phones.

Section 4.3 in the previous chapter outlines how NSO Group creates custom infrastructure for each customer. This unique, per-customer assignment is what allows attacks to be clustered and attributed: where the same infrastructure, for example an iCloud account, appears across multiple targets, those targets can be linked to the same Pegasus customer.

The forensic evidence from Amnesty International and independent findings from the French authorities show that many individuals selected in Pegasus Project records, both inside and outside Morocco, were ultimately infected with Pegasus using a common set of iMessage accounts (notably *bergers.o79[[@gmail.com](mailto:bergers.o79@gmail.com)]*). Amnesty International observed that many of these successful zero-click infections occurred just minutes after the target's phone number was *selected* or re-selected by the Moroccan customer in the Pegasus Project data.

The leaked records examined for the Pegasus Project do not extend into 2021, so it cannot be stated from those records alone that the system used against Moroccan targets in 2017–2019 was the same one used in the 2021 attacks. However, the forensic evidence closes that gap.

A number of individuals *selected* as targets by Morocco in 2019 were found to have been targeted again through 2020 and 2021. Claude Mangin, wife of jailed Saharawi activist Naâma Asfari, had her French number first *selected* in the DGST system in summer 2019. Forensic analysis shows her devices continued to be targeted and were infected from October 2020 through to July 2021.¹¹⁷ Forensic artifacts gathered from her devices confirm the 2020 and 2021 attacks were also carried out using iMessage accounts tied to the Moroccan Pegasus system. The same pattern was observed for other targets who appeared in the Moroccan customer Pegasus Project records and who continued to be targeted or compromised in the 2019 to 2021 period.

Amnesty International has previously published the set of Apple iMessage accounts used by Morocco to deliver Pegasus zero-click attacks between 2019 and 2021. Forensic records show clearly how the same set of iMessage accounts used by Morocco to target Moroccan and French journalists were also used to target French politicians and Sahrawi diplomats with Pegasus.

The French cyber-security agency ANSSI also performed extensive forensic investigations following the 2021 Pegasus Project revelations.¹¹⁸ In response to a *European Investigation Order* issued by the Spanish authorities, the French justice ministry sent a summary of technical evidence and indicators of compromise found by French investigators, which independently documented that same cluster of Pegasus Apple accounts used in the attacks, again tying back to Morocco.

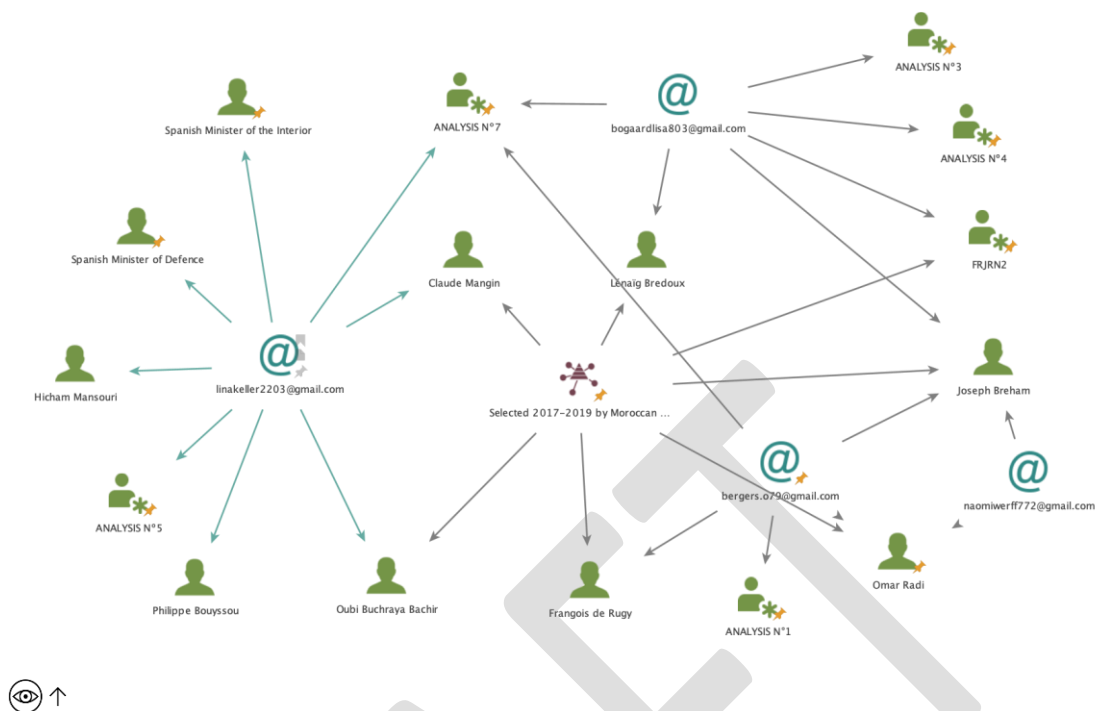
The same iCloud account used in 2021 against Claude Mangin and exiled Moroccan journalist Hicham Mansouri – *linakeller2203@gmail.com* – was also identified in a Spanish court document as the Apple account used in the 2021 Pegasus zero-clicks attacks which compromised the phones of the Spanish minister of interior and the minister of defence.¹¹⁹ The phone of Spain's prime minister was also compromised with Pegasus during the same time period in May-June 2021, but the court filings do not list the iMessage account used to infect his phone. The Spanish politicians were targeted with Pegasus in the midst of a diplomatic conflict with Morocco.¹²⁰

¹¹⁷ Amnesty International, *Forensic Methodology Report: Pegasus Forensic Traces per Target: Appendix D, see FRHRD Claude Mangin, 18 July 2021*, [amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/](https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/)

¹¹⁸ Ministerio Fiscal – Audiencia Nacional – Orden Europea de Investigación Pasiva núm. 15/2024. Número de Fiscalía, OEI 36/2024

¹¹⁹ estaticos-cdn.prensaiberica.es/epi/public/content/file/original/2023/07/10/15/2023-7-10-auto-archivo-caso-pegasus-pdf.pdf

¹²⁰ Amnesty International, "Spain/Morocco: People 'being used as pawns' as political games turn violent", 19 May 2021, <https://www.amnesty.org/en/latest/press-release/2021/05/spainmorocco-people-being-used-as-pawns-as-political-games-turn-violent/>



Graph showing connections between targets selected by Morocco and attack iMessage accounts

Table 1: Summary of iMessage accounts used in Pegasus attacks by Morocco

PEGASUS IMESSAGE ACCOUNT	TIMEFRAME	TARGET	ROLE	LOCATION	SOURCE
BERGERS.079[@]GMAIL.COM	2019	Omar Radi	journalist	Morocco	Amnesty
		Joseph Breham	lawyer	France	Amnesty
		Lénaïg Bredoux / ANALYSIS N°3	journalist	France	Amnesty & French authorities
		François de Rugy	politician	France	Amnesty
		ANALYSIS N°1			French authorities
NAOMIWERFF772[@]GMAIL.COM	2019-2020	ANALYSIS N°3			
		ANALYSIS N°7			
		Omar Radi	journalist	Morocco	Amnesty
		Joseph Breham	lawyer	France	Amnesty

PEGASUS IMESSAGE ACCOUNT	TIMEFRAME	TARGET	ROLE	LOCATION	SOURCE
BOGAARDLISA803[.]GMAIL.COM	2019-2020	Joseph Breham	lawyer	France	Amnesty
		Lénaïg Bredoux / ANALYSIS N°3	journalist	France	Amnesty & French authorities
		ANALYSIS N°4			French authorities
		ANALYSIS N°7			French authorities
LINAKELLER2203[.]GMAIL.COM	2021	FRJRN2	journalist	France	Amnesty
		Claude Mangin	human rights defender	France	Amnesty
		Philippe Bouyssou	politician	France	Amnesty
		Oubi Buchraya Bachir	diplomat	France	Amnesty
		Hicham Mansouri	journalist	France	Amnesty
		ANALYSIS N°5			French authorities
		ANALYSIS N°7			French authorities
		Spanish Minister of Defence			Spanish authorities
		Spanish Minister of the Interior			Spanish authorities

Taken together, the extensive technical and forensic evidence establishes three things. The DGST, the Moroccan Pegasus customer, began selecting individuals outside Morocco for Pegasus targeting from early 2018, among them activists, journalists, human rights lawyers supporting cases against Morocco, and family members of jailed activists.

Amnesty International forensically confirmed that a significant number of these people, located abroad and using non-Moroccan numbers, were in fact infected following selection in the Pegasus system.

The independent French and Spanish investigations found that the attacker accounts assigned to Morocco's Pegasus system, used against those Moroccan activists abroad, were the same accounts used to infect senior Spanish politicians' devices during the May–June 2021 diplomatic crisis with Morocco. Together these findings provide strong material evidence that Morocco was ultimately responsible for the extensive cross-border Pegasus surveillance campaign against critical journalists, activists, lawyers and politicians between 2019 and 2021.

6. OTHER DIGITAL SURVEILLANCE TECHNOLOGIES USED IN MOROCCO TO TARGET CIVIL SOCIETY

In addition to using Pegasus spyware as outlined in Chapter 5, the Moroccan authorities have also procured and used a broad range of digital surveillance tools from numerous countries over the past two decades, including the United States, Israel, France, Germany, the United Arab Emirates (UAE) and Italy. This chapter draws on previous reporting by digital security researchers alongside leaked Moroccan intelligence service materials that have been analysed by Amnesty International, as well as testimony from a former DSGT whistleblower, to provide a summary of how a range of different companies have supplied Morocco with sophisticated forms of both mass and targeted digital surveillance technologies.

The digital surveillance tools used by Morocco over the last two decades to target civil society include:

- The mass surveillance tool Eagle,¹²¹ acquired from French surveillance company Amesys in the early 2010s.
- The RCS (Remote Control System) spyware, developed by the now defunct Italian technology company Hacking Team, which was used in 2012 against members of the now-inactive Moroccan citizen media outlet Mamfakinch,¹²² and against other Moroccan journalists around the same time.¹²³ In 2015, emails included in a major leak from Hacking Team revealed that two Moroccan security agencies, the DGST and the National Defence Secrets Committee (*Commission du Secret de la Défense Nationale*, CSDN), had contracted with Hacking Team since at least 2009.¹²⁴

¹²¹ Jeune Afrique, “Espionnage : les anciens d’Amesys continuent leurs activités en Afrique du Nord” [Espionage: Former Amesys agents continue their activities in North Africa], 31 January 2020, <https://www.jeuneafrique.com/mag/886064/politique/espionnage-les-anciens-damesys-continuent-leurs-activites-en-afrique-du-nord/> (in French).

¹²² Privacy International, *Their Eyes on Me: Stories of Surveillance in Morocco*, April 2015, privacyinternational.org/sites/default/files/2018-02/Their%20Eyes%20on%20Me%20-%20English_0.pdf

¹²³ Committee to Protect Journalists, “Moroccan independent journalists describe climate of pervasive surveillance, harassment”, 1 July 2019, cpj.org/2019/07/moroccan-independent-journalists-describe-climate/

¹²⁴ Privacy International, “The right to privacy in the Kingdom of Morocco”, September 2016, uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=3915&file=EnglishTranslation

- The FinSpy spyware – developed by the British-German network of companies Gamma Group and FinFisher – which, in 2015, was identified by the Citizen Lab as operating in Morocco.¹²⁵ No specific customer or agency was publicly identified as the operator of FinSpy in Morocco.

Morocco was further identified as a customer of cyber intelligence company Cognyte, according to a December 2021 report from Meta on the surveillance-for-hire industry.¹²⁶ Cognyte, which was spun off in 2021 from US-based company Verint Systems, is a provider of cyber intelligence products including systems for internet and telecommunications interception. Cognyte claims to offer “software solutions” for governments to “neutralize and tackle threats to national security”.¹²⁷ Meta identified Morocco specifically as a customer of Cognyte’s social media monitoring product (previously known as WebintPro), which enables customers to control fake social media accounts (“avatars”) in order to gather intelligence about social media users or to launch social engineering attacks.

6.1 HACKING TEAM RCS SPYWARE (2009–2024)

The Moroccan DGST was among the biggest customers of the Italian Hacking Team RCS spyware, as revealed in emails and internal data leaked from the spyware maker in 2015.¹²⁸ Morocco was suspected in an early case of spyware misuse against civil society when Hacking Team’s RCS spyware was found to have been used in 2012 to target independent journalists in Morocco working with Mamfakinch.¹²⁹

The leaked internal Hacking Team material from 2015 included a detailed spreadsheet listing spyware customers alongside their internal code name, the customer contact point and any broker who facilitated the deal.¹³⁰ In the case of Morocco’s DGST, the initial 2012 sale was identified as being brokered by Al Fahad Smart Systems, also known as FSSys Tech, a UAE-based surveillance broker with a local entity in Morocco. The records also show that the DGST was licensed to infect up to 2,000 devices, with support for Windows, Mac and mobile devices.

Table 2: Sales of Hacking Team RCS to Moroccan agencies until 2015¹³¹

<u>CUSTOMER NUMBER</u>	6	36
<u>CODE</u>	CSDN	AlFahad
<u>CUSTOMER</u>	CSDN	Morocco - DST
<u>COUNTRY</u>	Morocco	Morocco
<u>KAM</u>	Maanna	Maanna
<u>AREA</u>	MEA	MEA
<u>AGENCY</u>	Intelligence	Intelligence
<u>CHANNEL OR DIRECT</u>	Direct	Channel
<u>PARTNER / FULFILLMENT VEHICLE</u>	Al Fahad	Al Fahad

¹²⁵ Privacy International, “Facing the truth: Hacking Team leak confirms Moroccan government use of spyware”, 10 July 2015, privacyinternational.org/blog/1394/facing-truth-hacking-team-leak-confirms-moroccan-government-use-spyware; Citizen Lab, “Pay no attention to the server behind the proxy: mapping FinFisher’s continuing proliferation”, 15 October 2015, citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

¹²⁶ Meta, *Threat Report on the Surveillance-for-Hire Industry*, 16 December 2021,

<https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf>

¹²⁷ Cognyte website homepage, <https://www.cognyte.com/> (accessed on 28 July 2026).

¹²⁸ The Hacking Team leaked files can be accessed on Wikileaks. Wikileaks, Hacking Team, 8 July 2015,

<https://wikileaks.org/hackingteam/emails/>.

¹²⁹ Ryan Gallagher, “How government-grade spy tech used a fake scandal to dupe journalists”, 20 August 2012, Slate, <https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html>;

Amnesty International, “How a hacking campaign helped shut down an award-winning news site”, 9 December 2016, <https://www.amnesty.org/en/latest/research/2016/12/how-a-hacking-campaign-helped-shut-down-an-award-winning-news-site/>

¹³⁰ Wikileaks, Hacking Team, 8 July 2015, <https://wikileaks.org/hackingteam/emails/>. The client overview list

<https://wikileaks.org/hackingteam/emails/>. The client overview list is email-ID 426797:

<https://wikileaks.org/hackingteam/emails/emailid/426797> <https://wikileaks.org/hackingteam/emails/>.

<https://wikileaks.org/hackingteam/emails/emailid/426797>

¹³¹ Wikileaks, Hacking Team, 8 July 2015. <https://wikileaks.org/hackingteam/emails/>. The client overview list is email-ID 426797:

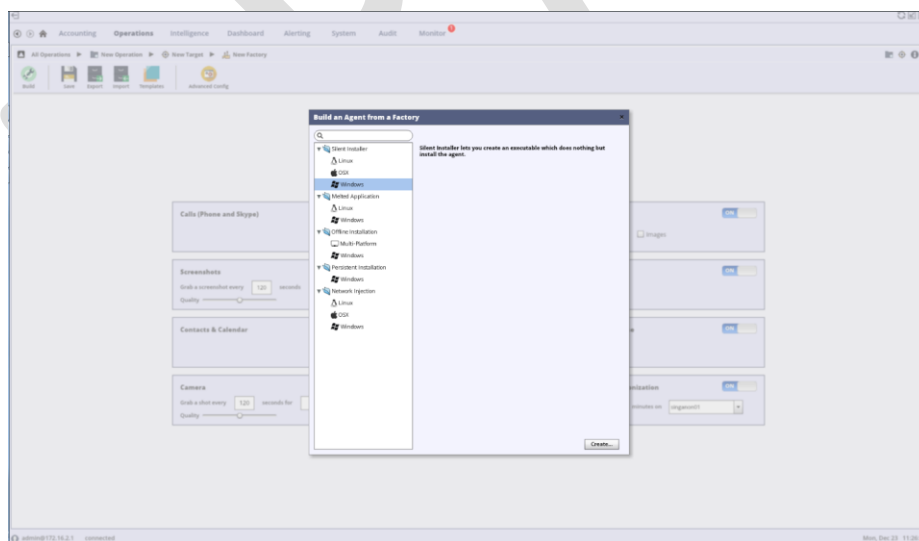
TOTAL # TARGETS	300	2000
YEAR BOUGHT FIRST RCS	2009	2012
EXPLOIT	Yes	No

The leak of these files led to a crisis among the secretive customers purchasing Hacking Team's spyware, with many governments ending their relationship and seeking out new vendors such as the emerging NSO Group.¹³² In response, Hacking Team restructured, was acquired by InTheCyber group, and was renamed Memento Labs.¹³³

According to an interview with Paolo Lezzi, the chief executive of Memento Labs, Hacking Team had just three remaining government customers in 2019.¹³⁴ Morocco continued to receive software updates and new licences for the spyware long after the 2015 leak: based on leaked Moroccan intelligence documents reviewed by Amnesty International, Morocco received updates until at least 2020, suggesting that its contract continued with Memento Labs after the company's restructuring.

The Hacking Team system operated by the DGST was code-named PIACENZA, as noted in the leaked Moroccan intelligence files analysed by Amnesty International. This material included code, licences, documentation and other material related to the DGST's use of the Hacking Team spyware. These documents and leaked Moroccan intelligence files show that Morocco deployed the upgraded RCS X system after 2018, which was still licensed for use against 2,000 unique devices. The licence included support for Windows, Mac, iOS, Android and BlackBerry, but not Linux or Windows phones. A surveillance system collecting data from hundreds or even thousands of devices would require significant human resources to review, process and analyse the collected data, and the RCS licence shows that the system was also licensed for use by up to 80 internal users (analysts and operators).

In addition to licensing information, Amnesty International also reviewed leaked RCS product documentation, internal records from the DGST's Hacking Team deployment, system screenshots and surveillance records, in order to verify Morocco's use of the spyware system.

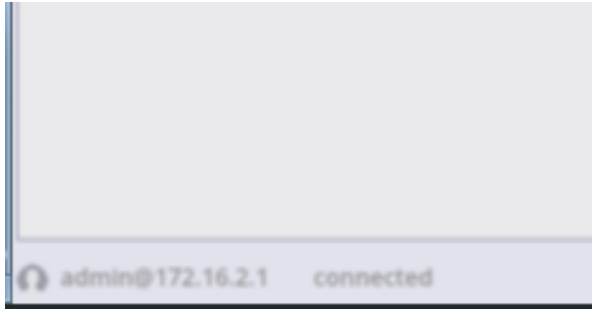


Screenshot of internal spyware control panel for the DGST (Source: leaked internal DGST material)

¹³² Lorenzo Franceschi-Bicchierai, "Hacking Team is back in business, but struggling to survive", 24 March 2016, Vice, <https://www.vice.com/en/article/hacking-team-is-back-in-business-but-struggling-to-survive/>

¹³³ Raffaele Barberio, "Cyber-intelligence, nasce Memento Labs dalla fusione delle attività di InTheCyber Group e la storica Hacking Team" ["Cyber-intelligence, Memento Labs is born from the merger of the activities of InTheCyber Group and the historic Hacking Team"], 2 April 2019, Key4Biz, <https://www.key4biz.it/cyber-intelligence-nasce-memento-labs-dalla-fusione-delle-attivita-di-inthecyber-group-e-la-storica-hacking-team/252368/> (in Italian).

¹³⁴ Lorenzo Franceschi-Bicchierai, "CEO of spyware maker Memento Labs confirms one of its government customers was caught using its malware", 28 October 2025, TechCrunch, <https://techcrunch.com/2025/10/28/ceo-of-spyware-maker-memento-labs-confirms-one-of-its-government-customers-was-caught-using-its-malware/>

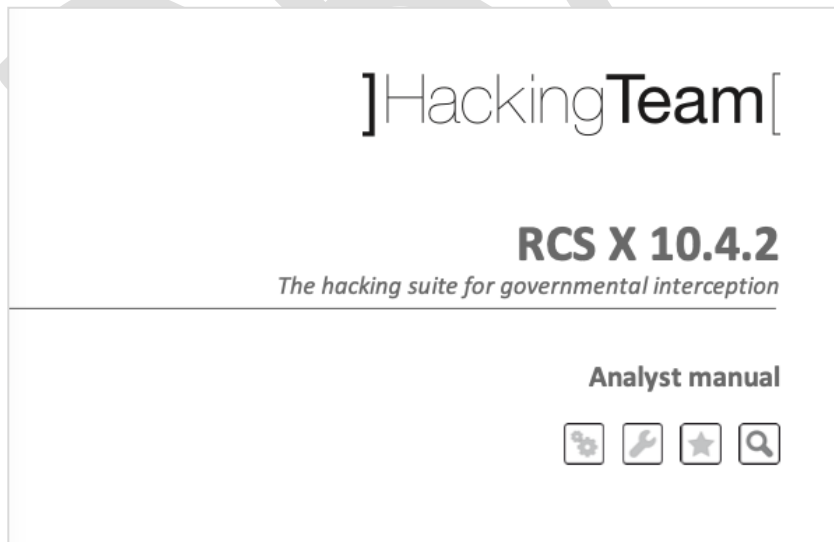


Zoomed in detail showing the IP range.
(Source: leaked internal DGST material)

Internal screenshots from the RCS system show that it was being operated on an internal subnet with the IP range 172.16.2.0/24. Notably, this internal IP range has been previously linked to Hacking Team activity. A 2018 report from security researchers at the cybersecurity company ESET identified four updated Hacking Team RCS samples communicating with a command and control server (see glossary) at 172.16.1.206.¹³⁵ This is the same IP range as the Moroccan RCS system, showing that the system was being used to actively generate new RCS spyware samples from 2015- 2017. Most likely these samples were generated for internal testing and configured to communicate directly to the internal command and control server rather than being routed through the RCS anonymizing proxy servers. ESET's independent technical findings confirm that Morocco's Hacking Team system continued to be used after the 2015 Hacking Team breach, consistent with the recently leaked Moroccan intelligence service materials reviewed by Amnesty International.

6.2 PHYSICAL INFECTION OF DEVICES

Safir told Amnesty International that the DGST routinely took advantage of occasions when they would have physical access to the devices of targets to infect them with malware; for example, when targets were transiting airports. Amnesty International has confirmed that the devices of journalists and human rights activists were targeted with physical infection. A non-public 2019 manual for Hacking Team's RCS X system, reviewed by Amnesty International as part of the leaked Moroccan intelligence service materials, describes the physical infection vectors available for Windows and Android.



Cover of the leaked 2019
Hacking Team RCS manual.¹³⁶

¹³⁵ Filip Kafka, "New traces of Hacking Team in the wild", 9 March 2018, WeLiveSecurity, <https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/>

¹³⁶ Image taken from leaked Morocco intelligence files reviewed by Amnesty International.

Infection methods

A device can be infected via:

- **physical infection:** the device is infected by the execution of a file transmitted using USB memories, CDs or documents. Evidence can be collected physically or via Internet as soon as the device connects;
- **remote infection:** the device is infected by the execution of a file transferred via Internet connection or made available in a Web resource. Evidence can be collected physically or via Internet as soon as the device connects. Remote infection can be enhanced using Network Injector.



Physical and remote infection vectors (leaked Hacking Team manual)

According to the manual, on Windows devices, physical infection can be achieved via opening a silent executable or by booting into an RCS installer to install the spyware pre-boot. On Android devices, the RCS spyware can be installed through physical access via opening a silent APK (see glossary), or by installing through booting into an Android recovery image on supported devices.

List of installation vectors

Installation vector descriptions

Following is a list of vectors with supported device types and operating systems:

Installation Vector	Device	Operating system	Description
Installation Package	Mobile	Android, BlackBerry, iOS.	Creates an auto-installer file with the agent.
Local Installation	Mobile	BlackBerry, iOS.	Installs the agent on the target device either through USB or SD/MMC memory card.
Melted Application	Desktop Mobile	Linux, Windows Android.	Adds the agent to any application file.
Network Injection	Desktop	Linux, OS X, Windows	Link to the injection rule creation page. See " Managing the Network Injector " on page 65.
Offline Installation	Desktop	Multiplatform Windows.	Creates an ISO file to generate a boot CD/DVD/USB to be used on computer that is off or hibernating
Persistent Installation	Desktop	Windows	Adds the agent to the target computer's firmware.
QR Code/Web Link	Mobile	Multiplatform, Android, BlackBerry.	Generates a QR code or Web link that, once processed by the target device, will allow the agent to be downloaded.
Silent Installer	Desktop	Linux, OS X, Windows	Creates an empty executable file that, when run on the target device, installs the agent.
SMS Message	Mobile	Multiplatform, Android, BlackBerry.	Sends a SMS message that installs the agent if the target opens its content.
Wap Push Message	Mobile	Multiplatform, Android, BlackBerry.	Sends a WAP message that installs the agent if the target opens its content.

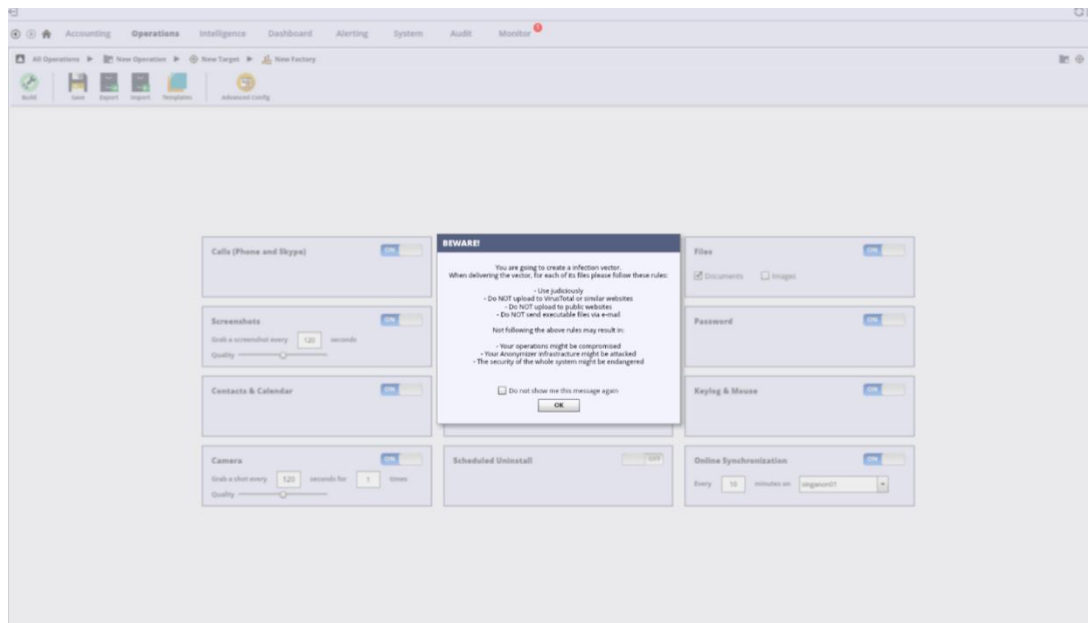


List of Hacking Team infection vectors from May 2019 (RCS X 10.4.2)¹³⁷

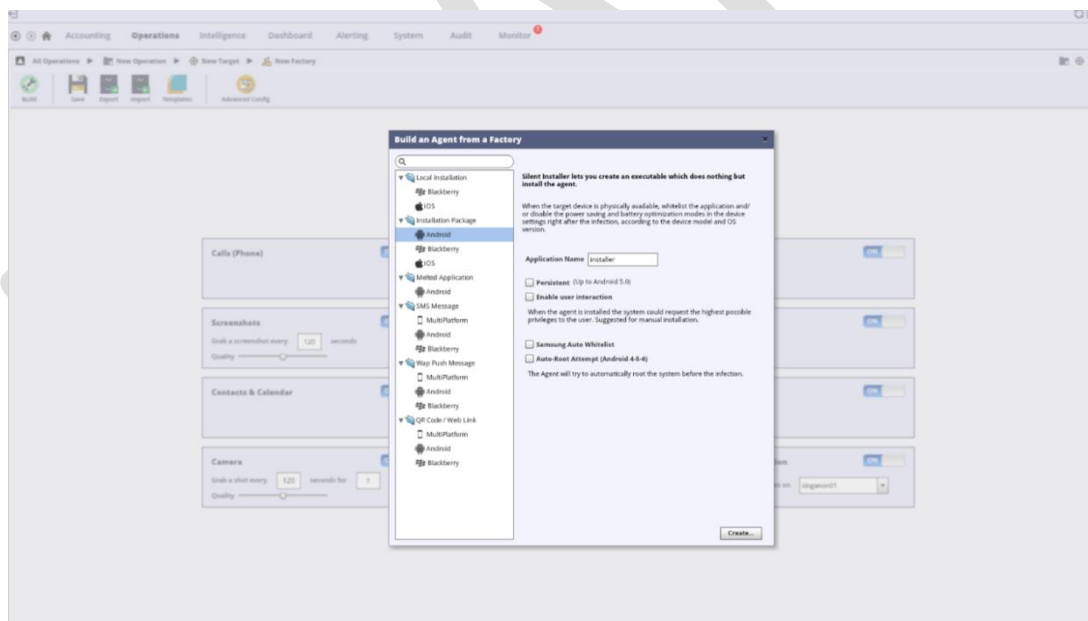
Technician manual | ver.C_MAY-2019 | RCS X 10.4.2 | 2018© HT S.r.l. - page 133

¹³⁷ The technical manual is part of the leaked Morocco intelligence files reviewed by Amnesty International.

The Hacking Team RCS dashboard allows non-technical surveillance operators to prepare USB keys designed to automatically infect Windows computers with the spyware.



Screenshot of interface for preparing a Windows spyware infection on the Moroccan Hacking Team system. [Source:](#)



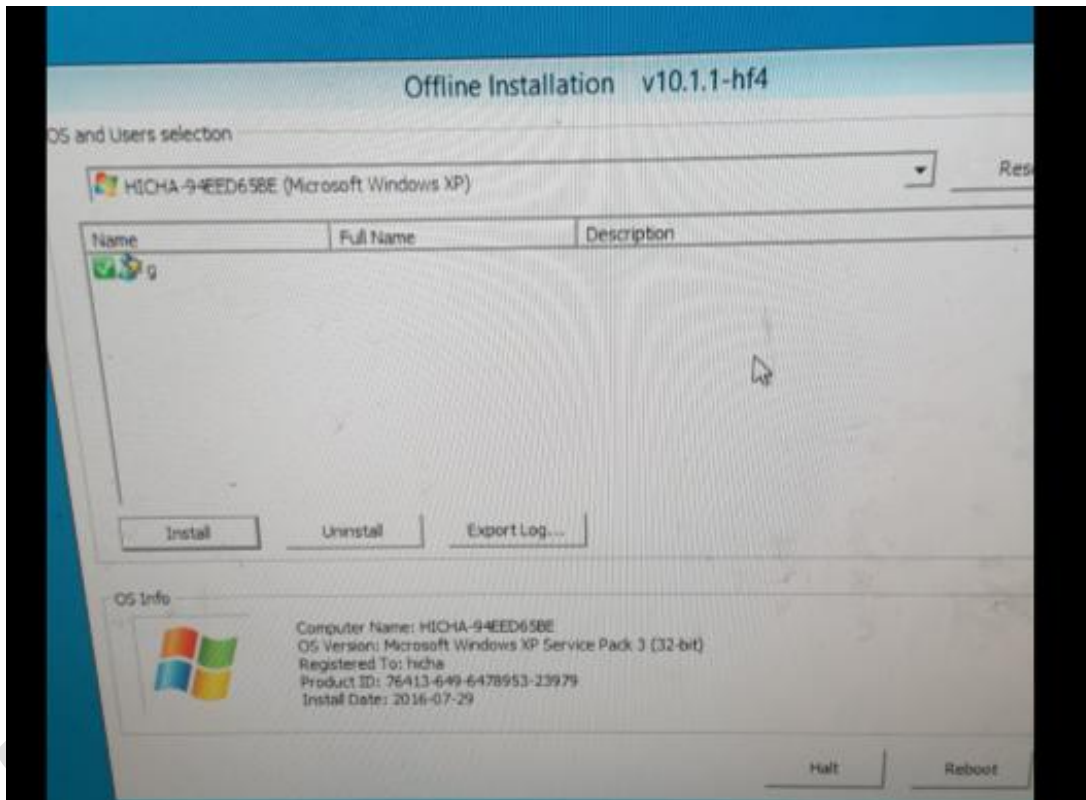
Screenshot of interface for preparing a Windows spyware infection on the Moroccan Hacking Team system.

With the USB prepared, a field operator simply needs to connect the USB stick to the target computer and boot into the RCS spyware installer. The installer prompts the operator to confirm the infection and then handles the steps needed to infect the computer. From start to finish the process takes less than 30 seconds, fast enough that it could be performed inconspicuously with temporary access to the computer. Such physical infection vectors would likely have become more difficult as Windows Secure Boot and

Bitlocker encryption became more widely supported on end-user PCs. Windows Secure Boot has been mandatorily enabled by default on PCs since the launch of Windows 11 in 2021.

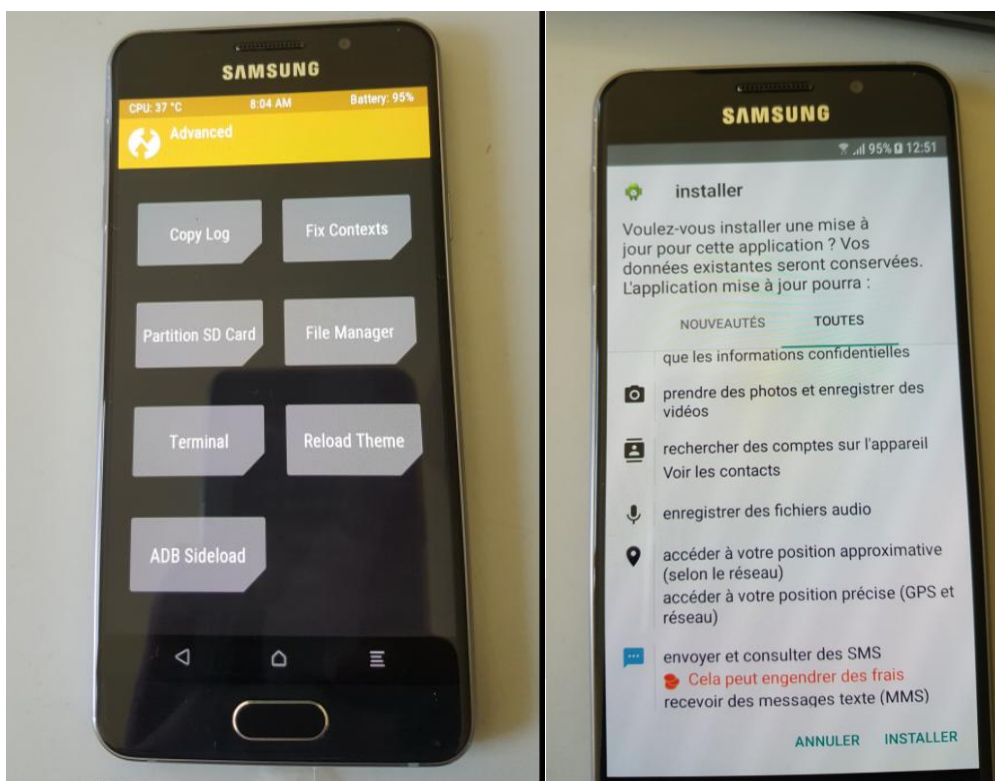
According to *Safir*, the tactic of pre-infecting computers in specific internet cafes was particularly important during the 2016-2017 Hirak El-Rif protests:

“We infected so many internet cafés with RCS [spyware]. The field agents tell us which cyber café the target is visiting, and we had visibility on what they were doing because we had previously infected all the machines there. Even when the [Hacking Team] contract ended, we were able to continue the operations on the cyber cafés and receive the data from the infected machines on our end. I made video tutorials for colleagues in the field to train them in how to infect the workstations in the cyber cafés. We gave USB sticks to every unit in each neighbourhood with operation codes for each city. That’s the offline installation of the RCS agent on PCs.”



Screenshot of installation of Hacking Team RCS Windows agent on an internet café PC in Morocco.

A similar approach could be used to prepare an RCS infection payload for installation on a mobile phone when the operator had physical access to it.



Installation of Hacking Team RCS agent on an Android phone via the recovery system.

The physical infection process could also be used to infect “new” devices, which would then be covertly provided to targeted individuals via “agents” collaborating with the DGST, for example vendors at second-hand phone shops. In such cases, the phone would appear to the target to be new and unused; however, it would provide the authorities with full access to their device, their communications and data on their immediate environment. The RCS Android spyware allowed the operator to track the target’s location, take photos from the front and rear cameras, activate the microphone and log all communications and activity on the device.

Safir described how, at the time of the 2016-17 protests in the Rif region, intelligence agents would identify a second-hand phone shop where targets bought their devices and arrange with the merchants to give phones pre-infected with RCS spyware to “people active in the Hirak [protest movement]”.

“Back then Samsung S6 Edge was trendy. We bought around 50 phones that we aimed to deliver. We give the infected phones to the shop owners and they go to the targets, because they trust them, and tell them, ‘I have this brand new phone for you’. We rooted the phones [bypassed manufacturer restrictions to gain administrator-level controls] beforehand and installed a custom recovery containing a pre-installed RCS agent.”

According to *Safir*, a local telecommunications provider would also provide network access to certain targets, including prominent Hirak El-Rif activists.

Surveillance material reviewed as part of this investigation confirmed the methodology described by *Safir*. A particularly revealing photograph – taken by Hacking Team’s RCS spyware – captures an activist based in Morocco’s Rif region as they are unboxing a new phone. The front-facing camera took an image of what looks to be a recently opened and empty Samsung Galaxy S6 Edge phone box. Simultaneously, the rear-facing camera surreptitiously took a photo of the phone’s new owner, the first photos from that spyware victim.

The photo was taken in April 2017 during Morocco’s crackdown on the Hirak El-Rif movement. The evidence suggests the phone was already infected with the RCS spyware before it was unboxed by the target.

Amnesty International and media partners identified the activist based on information in the surveillance records. The individual said that they were active in the local protest movement at the time, and that the phone was obtained from a vendor in Al Hoceima. The activist was not a prominent member of the protest movement at the time, indicating that the Moroccan authorities were comfortable spreading infected devices widely to gather intelligence on the protest movement.



Phone unboxing captured by the DGST's Hacking Team spyware system. Leaked Moroccan intelligence files

Safir recalled:

“What we were doing was taking smartphones, installing Trojans [malicious software], and then resetting the phone to its factory state, as if the phone was coming out of the box [for the first time]. When you turn it on, it asks you to choose the language and you think it’s new. Actually, he’s already trapped... Psychologically, it works very well.”

6.3 IMSI CATCHERS

According to *Safir*, for calls and mobile data not directly accessible through telecommunications providers, DGST agents have recourse to IMSI catchers, also known as cell site simulators or “Stingrays”.¹³⁸ These are designed to imitate a mobile phone tower in order to identify nearby phones and intercept calls or data in real time, and can also catch the data from nearby devices, including from encrypted messaging apps prior to transit.

“We only had three or four IMSI catchers for the DGST. So we had to manage with different techniques when we did not have access to the tools. [The telecommunications provider] put us in the same network as the target and

¹³⁸ Business and Human Rights Centre, “Hidden risk is the most expensive: What investors need to know about high-risk surveillance technology”, 28 January 2026, <https://www.business-humanrights.org/en/from-us/briefings/hidden-risk-is-the-most-expensive-what-investors-need-to-know-about-high-risk-surveillance-technology/>

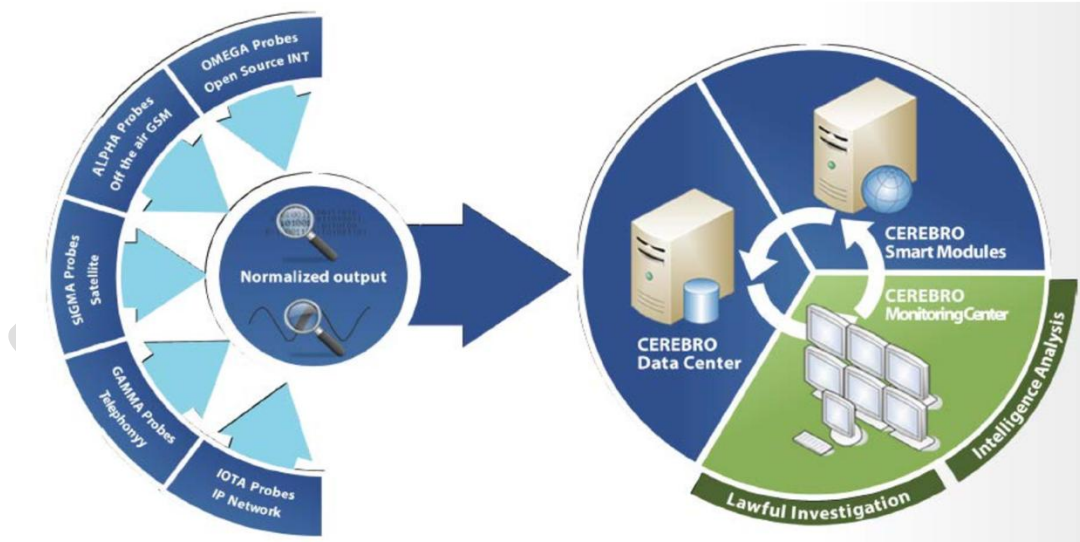
we ‘man-in-the-middle’ [a technique that allows an attacker to read, modify or block a target’s traffic]. Sometimes we even got access to the Wi-Fi routers. They even did this with the activists of the 20 February movement [a mass protest movement that began in 2011 as part of the Arab Spring]. The telecommunications provider became used to these requests from the DGST. We called them by phone and we told them what we needed in terms of access and they obliged.”¹³⁹

6.4 MASS SURVEILLANCE TECHNOLOGIES

In addition to targeted surveillance technologies, Morocco has also used a number of mass surveillance technologies which allow for the widespread and bulk monitoring, interception, storage or analysis of user materials. Such systems facilitate violations of the right to privacy and also create a chilling effect in society, whereby people are deterred from exercising their rights, both online and offline.

6.4.1 EAGLE / CEREBRO MASS INTERNET SURVEILLANCE SYSTEM

French telecom and defence company Amesys was a supplier of mass communication interception technologies to the Moroccan government in the early 2010s.¹⁴⁰ Amesys developed and sold a monitoring system called Eagle, capable of performing mass surveillance of internet traffic at the scale of a whole country. Amesys ceased its activities in the cyber-surveillance sector in 2012, after the transfer of its assets to Nexa Technologies, which renamed Eagle as Cerebro.¹⁴¹



Architecture of Cerebro mass surveillance system. Amnesty International has previously provided a more detailed analysis of Cerebro as part of the Predator Files investigation.¹⁴²

The human rights risks of such powerful mass surveillance technologies were highlighted in June 2021, when four executives from Nexa Technologies (part of the Nexa group of companies) and Amesys were indicted on suspicion of complicity in torture by a French court after selling their surveillance technology to the Libyan and Egyptian governments that was then used to track down opponents, who were then arrested

¹³⁹ Interview with *Safir*.

¹⁴⁰ Jeune Afrique, “Espionnage : les anciens d’Amesys continuent leurs activités en Afrique du Nord” (previously cited).

¹⁴¹ Amnesty International Security Lab, “Predator Files: technical deep-dive into Intellexa Alliance’s surveillance products”, 6 October 2023, securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/

¹⁴² Amnesty International Security Lab, “Predator Files: technical deep-dive into Intellexa Alliance’s surveillance products” (previously cited).

and tortured in jail.¹⁴³ The indictments were cancelled one year later by the Paris Court of Appeal, though the investigation was not closed.¹⁴⁴

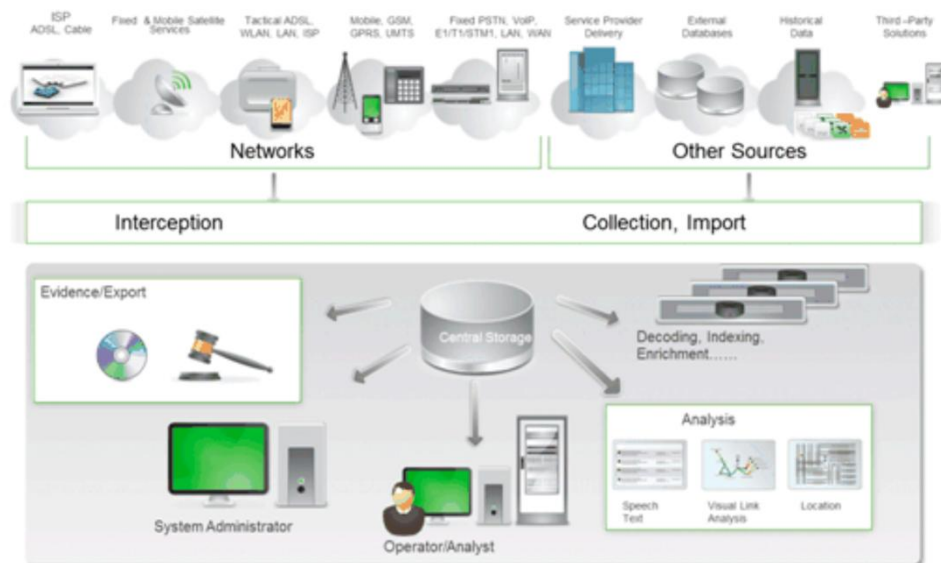
Internal records from Amesys and the Nexa group confirm that a sale of the mass surveillance technology to Morocco was agreed in December 2009. The project, code-named “Popcorn” by Amesys, involved the deployment of the Eagle/Cerebro mass internet interception technology in Morocco. The company records indicate that Morocco paid more than €7.5 million (\$8.7 million) for the technology.

6.4.2 MAGAZINE: VERINT SUPPLIES LARGE SCALE INTERCEPTION SYSTEMS TO MOROCCO

In 2022, the hacker group “LeakTheAnalyst” released gigabytes of internal emails they claimed were from the US company Verint which included specific email accounts of people working in Verint’s cyber intelligence divisions (later spun out as Cognyte). The data was already historical at the time of publication, mostly pre-dating 2017.

Amnesty International reviewed a copy of the leaked material, including confidential spreadsheets tracking the progress of product sales opportunities. Among the data are many sales proposals to Morocco, which was code-named “Magazine” in the document, as is apparent from references to Maroc Telecom and other Moroccan telecom operators in certain “Magazine” proposals. (see Annex 12.2).

The internal Verint records show that it closed a sale, to a Moroccan (“Magazine”) customer code-named “Canelle” for \$14 million in December 2014. The records state the sale was of Verint’s Reliant 12 system, which allows for the unified collection and analysis of telephone communication, mobile internet service providers (ISPs) and internet traffic data.



Architecture of Verint's Reliant product (Leak Verint Reliant manual)

¹⁴³ Amnesty International, “Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture”, 22 June 2021, [amnesty.org/en/latest/press-release/2021/06/executives-of-surveillance-companies-amesys-and-nexa-technologies-indicted-for-complicity-in-torture/](https://www.amnesty.org/en/latest/press-release/2021/06/executives-of-surveillance-companies-amesys-and-nexa-technologies-indicted-for-complicity-in-torture/)

¹⁴⁴ Tech Xplore, “Charges dropped against French company over Egypt spyware”, 14 December 2022, <https://techxplore.com/news/2022-12-french-company-egypt-spyware.html>

In October 2016, the sales records show that Verint closed the sale of an upgrade of the Reliant system, expanding their offering to support up to 100 Gbit/s of internet communications traffic. Until 2017, when the leaked Verint data stops, Verint continued to pitch new products to their Moroccan “Canelle” customer including “EPI Premium”. EPI refers to “End Point Interception” which Amnesty International identifies as Verint’s term for their spyware product which was being developed and sold at that time. Verint records indicate that the EPI product had capabilities to infect both Windows and Android devices.¹⁴⁵ Cognyte, Verint’s cyber-intelligence spin-out company, was reported to have closed its ACE Labs division in 2022 which developed Cognyte’s cyber intrusion products.¹⁴⁶ There is no indication in the records that the EPI product was ultimately sold to Morocco.

¹⁴⁵ Internal Verint records also refer to the EPI products using the terms ROCKstar and ROCK*. Both the Android and Windows components have previously been observed in-the-wild, but were not publicly attributed to Verint.

¹⁴⁶ Meir Orbach, “Offensive cyber company ACE Labs closing down”, 14 June 2022, Calcalist, <https://www.calcalistech.com/ctechnews/article/skywpqy9>

7. UNLAWFUL SURVEILLANCE: TOOLS AND TECHNIQUES IN PRACTICE

“There are written laws but they don’t apply. There are laws that no one respects. They don’t care about judicial authorization, warrants. Sometimes you can even a posteriori draw up the documents, do things in reverse. There’s complete impunity. We start with the verdict.”

Safir

The previous chapters outline new evidence on the range of digital surveillance technologies that have been used in Morocco. This chapter presents an overview of how surveillance against civil society works in practice.

Once a person is marked as a surveillance target, the DGST has an array of tools at its disposal, including advanced targeted and mass surveillance technologies detailed in Chapter 6. However, based on *Safir’s* testimony, the authorities for the most part rely on more traditional methods, such as analogue tools and less sophisticated technologies. This is reliant on individual agents, phone tapping with DGST agents transcribing calls, wiretapping of homes or even cars, and/or payment or threats to neighbours, friends or other informants to report to the DGST. However, it may also involve complex systems woven into the communications infrastructure of the entire country. While each of these methods is invasive in its own right, when used in combination they constitute a “surveillance ecosystem”¹⁴⁷, which creates a near total web of surveillance of every aspect of a target’s physical and digital life from which it is almost impossible to escape. This unlawful surveillance is directly in conflict with international human rights law and standards.

The objective of surveillance operations targeting human rights defenders is often to silence the target, to destroy or sully their reputation, or gather enough information to serve as the basis for judicial harassment or criminal prosecutions. Such operations targeting an individual human rights defender or journalist include

¹⁴⁷ OHCHR, *Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights*, 21 April 2026, UN Doc. A/HRC/62/45.

multiple tactics which vary according to the target, their circumstances, gender and “importance”.¹⁴⁸ *Safir* explained to Amnesty International that these operations are not time-limited: “it’s a job that lasts until we have something”.¹⁴⁹

According to *Safir*, the use of spyware, especially high-cost foreign-sourced tools such as Pegasus, is treated as a last line of attack, only after the low-tech option of “listening” fails to provide the desired data. He explained:

“Once we have arrived at Pegasus, we have taken all the other steps. It comes after the tapping, in their apartment, in their car. It’s a scientific thing, as we say”.

In other words, spyware was only used when other methods collectively proved insufficient for the most “sophisticated and well-known” targets or, as in the cases of Omar Radi and Maâti Monjib (detailed below), to trial a new surveillance technology. *Safir* described the methodological organization of Omar Radi’s WhatsApp contacts (“Desk”, “Friends”, “Project”) which saved the agents time when classifying the data. In an interview with Amnesty International, Omar Radi confirmed that his contacts were stored on his device in this manner, saying, “I organize my contacts like any journalist”.¹⁵⁰

CASE STUDY: MAÂTI MONJIB

“Him, he was a test.”

A “guinea pig”¹⁵¹ is how *Safir* summed up the targeting of political activist and former prisoner of conscience Maâti Monjib with Pegasus in 2017 – one of the first people to be targeted with the spyware.

According to *Safir*, Maâti Monjib was targeted for two reasons. First, he was considered to be one of the most prominent and long-standing human rights defenders in Morocco. Second, he was in close contact with journalist Omar Radi. In 2017, when Pegasus was being rolled out in Morocco, it was used alongside other less sophisticated and more traditional methods of surveillance, including physical tailing and planting cameras and microphones.

Maâti Monjib, who still lives in Morocco, refers to the period from 2015 to 2019 as the time when he felt the most oppressive force of state repression, including judicial harassment and surveillance. For example, in 2015 the Moroccan authorities brought bogus charges against him and six other defendants for receiving foreign funds from the NGO Free Press Unlimited, money used to conduct training sessions for citizen journalists. Again in December 2020, Maâti Monjib was arrested after a Rabat court convicted him of “threatening the internal security of the state”.¹⁵² One month later, a different court sentenced him in his absence to one year in prison for the case dating back to 2015.¹⁵³ Amnesty International called for his immediate release and designated him a prisoner of conscience.¹⁵⁴ He was released in March 2021 but the charges against him were not dropped.¹⁵⁵

Since then, he has continued to face the authorities’ silencing tactics.

“The surveillance is less intense now [than during 2015-2019] but it’s still psychologically very harmful for me and my family. My daughter had to leave Morocco when she was 16 because of all the repression that I was subject to. My wife, who is French, was sacked from her job in January 2020 at an NGO because of me.”

The royal pardon he received in July 2024 has had no positive impact on his situation in Morocco. He has not been able to return to his job as a university professor, he is subjected to a travel ban, his assets remain frozen, and he is regularly subjected to smear campaigns.

¹⁴⁸ « Ça dépend de son importance », interview with Amnesty International.

¹⁴⁹ Interview with *Safir*.

¹⁵⁰ Interview in person with Omar Radi, April 2026, France.

¹⁵¹ “Maâti Monjib a servi de cobaye initial”

¹⁵² Amnesty International, “Morocco: Prisoner of conscience provisionally released: Maâti Monjib” (Index: MDE 29/4377/2021), 6 August 2021, <https://www.amnesty.org/en/documents/mde29/4377/2021/en/>

¹⁵³ Amnesty International, “Morocco: Imprisoned academic’s life in danger: Maâti Monjib” (Index: MDE 29/3863/2021), 19 March 2021, <https://www.amnesty.org/en/documents/mde29/3863/2021/en/>

¹⁵⁴ Amnesty International, “Morocco: Academic arbitrarily detained: Maâti Monjib” (MDE 29/3481/2021), 5 January 2021, <https://www.amnesty.org/en/documents/mde29/3481/2021/en/>

¹⁵⁵ Amnesty International, “Morocco: Prisoner of conscience provisionally released: Maâti Monjib” (Index: MDE 29/4377/2021), 6 August 2021, <https://www.amnesty.org/en/documents/mde29/4377/2021/en/>

“I had nothing to be pardoned for,” he told Amnesty International. “A pardon implies you did something wrong.”¹⁵⁶

Safir explains that the process of targeting individuals begins at the operational level, with “finding their weaknesses”, or “finding a reason” to justify an arrest – no matter how small. The “listening” stage is critical for this. He explained: “For example, we’ll look to see if you like women, or drinking, or gambling. We need to really know you... to know if there is something hidden”. This process can incorporate bribes or blackmail. He added:

“With the journalists, the beginning is whether we can buy them or not. There aren’t many people who resist money. Or if we can manipulate them, with a girl for example. If it’s someone who drinks a lot, we can present a negative image to the Moroccan people. Afterwards, the technical stuff is easy. Most people share their number. They don’t know how to protect themselves.”¹⁵⁷

If the target is a woman, this process can play on heteropatriarchal norms and legal restrictions in Morocco, such as laws criminalizing extra-marital sexual relations and access to abortion.¹⁵⁸ “It’s simpler because in Morocco it’s not normal for a single woman to have a lover, not for her family, not for society... It’s scandalous to think they have a relationship outside marriage,” *Safir* explained.

This targeted harassment of HRDs continues even when they have left Morocco. For example, even while living in the USA, the journalist and activist Afaf Bernani has been subjected to manipulated images of her, including an explicit video of her and Taoufik Bouachrine [see case study: Afaf Bernani in Chapter 8], and sexualized and abusive messages on social media posts. “My body was weaponized,” she told Amnesty International. “Sexual degradation replaced conventional defamation.”¹⁵⁹

7.1 TARGETING FAMILY AND NETWORKS

Once an individual human rights defender or journalist becomes a subject of investigation, members of their families and networks can also become ensnared in the operation. The simple fact of being in contact with a target can turn others into surveillance targets too. As *Safir*, explained: “If you, a woman, know [a target] and you keep calling them, voilà, that’s someone close to you. We can switch directly to you.”¹⁶⁰

One example of this was journalist Omar Radi, who *Safir* confirms was considered a priority threat by the authorities due to his popularity and his independent journalism, which was often critical of the authorities. Omar Radi was aware that surveillance extended to his wider social circle. He told Amnesty International of “the disproportionate resources used to surveil me, punish me, trap me”. This was separately confirmed by *Safir*. Omar Radi also told Amnesty International of times when his family members noticed they were being physically followed, including his mother.¹⁶¹

Safir told Amnesty International that Omar Radi’s mother was followed when going about her daily activities and her phone was tapped. His brother and other relatives and friends were also watched, and their historical phone calls checked retroactively. Even the man from whom he bought his cigarettes was placed under surveillance. All calls were transcribed verbatim by agents from the DGST’s Directorate of Operational Surveillance (DSO) in case a code was being used: “every sigh, every cough, every ‘ah’,” as *Safir* put it.¹⁶²

Omar Radi also knew that some acquaintances and sources were approached for information, and he paid tribute to those who refused to comply: “It doesn’t surprise me. But there have also been lots of people, many, many neighbours, the corner grocer, the caretaker, the street guard, etc., who were offered money to take pictures of me or to share details of my life and who said no.”¹⁶³

¹⁵⁶ Interview by phone with Maâti Monjib, December 2025.

¹⁵⁷ Interview with *Safir*.

¹⁵⁸ See, for example, the case of the arrest of Hajar Raissouni, a journalist who was arrested along with her fiancée coming out of a doctor’s office and sentenced to one year in prison for “having an abortion and sex outside marriage,” both crimes under Moroccan law; Amnesty International, “Morocco: One Year In Prison For Unlawful Abortion: Hajar Raissouni” (Index: MDE 29/1131/2019), 3 October 2019, <https://www.amnesty.org/en/documents/mde29/1131/2019/en/>

¹⁵⁹ Interview by phone with Afaf Bernani, March 2026.

¹⁶⁰ Interview with *Safir*.

¹⁶¹ Interview in person with Omar Radi, April 2026, France.

¹⁶² Interview with *Safir*.

¹⁶³ Interview in person with Omar Radi, April 2026, France.

CASE STUDY: OMAR RADI

"We found nothing on Omar Radi. Nothing." – *Safir*¹⁶⁴

In June 2020, Amnesty International forensically confirmed that Moroccan journalist and activist Omar Radi was targeted by the Moroccan authorities using Pegasus spyware. Following publication, a media harassment campaign was launched against Amnesty International in an attempt to discredit the organization's findings and distract attention from the state's unlawful surveillance of human rights defenders and journalists.¹⁶⁵

Within weeks of Amnesty's publication revealing his Pegasus infection, Omar Radi was arrested, subjected to questioning and, in July 2020, detained pending trial on charges of "harming national security", "sexual assault" and "rape". He was held in pretrial detention from July 2020 until July 2021, when he was convicted and sentenced to six years in prison in July 2021 in a trial marred by due process violations.¹⁶⁶

The indictment in both the espionage and rape cases, dated 18 March 2021, confirms that the authorities had kept the journalist under surveillance since 29 December 2017. This surveillance had been accompanied by regular defamatory campaigns against him via Moroccan news websites.¹⁶⁷ Omar Radi was released following a royal pardon in July 2024.

In an interview with Amnesty International, when discussing why he was considered a priority target by the authorities, Omar Radi concluded: "I think that, after my first arrest,¹⁶⁸ they saw the extent of the sympathy and solidarity with me. And they said to themselves, this is a potential danger in the future, it would be better to deal with this threat urgently and break it."¹⁶⁹

Safir's testimony confirms the exceptional, almost obsessive, level of state surveillance and harassment deployed against Omar Radi since the 20 February Movement in 2011.¹⁷⁰ In addition to NSO Group's Pegasus spyware, *Safir* told Amnesty International that the authorities used IMSI catchers to intercept his calls, forensic surveillance tool Cellebrite UFED to break into his phone, and hidden microphones and cameras. This was combined with physical surveillance and phone tapping (of both Omar Radi and his family), media harassment, physical assault,¹⁷¹ and criminal investigation and prosecution. Personal details provided to Amnesty International by *Safir* were confirmed by Omar Radi; for example, that he drove a black Dacia Sandero car, as well as the description of a close friend's car.

Far from making him angry, Omar Radi told Amnesty International that the revelations in this report, particularly those from *Safir*, make him determined to continue fighting against abuse of power and repression:

"The state and especially the security apparatuses are becoming more and more barbaric, more and more inhuman. We have a society that wants to move forward but is prevented by the security apparatus. And this situation really needs to change."

The media harassment campaigns against him continue to the present day.¹⁷² Omar Radi also believes that he continues to be subject to surveillance, despite currently living overseas:

¹⁶⁴ Interview with *Safir*.

¹⁶⁵ Amnesty International, "Morocco and Western Sahara: Government smear campaign against Amnesty International underlines intolerance of scrutiny" (previously cited).

¹⁶⁶ Amnesty International, Urgent Action, Morocco Further information: Detained journalist must get a fair trial: Omar Radi, 26 January 2022, <https://www.amnesty.org/en/documents/mde29/5184/2022/en/>

¹⁶⁷ As detailed in Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited).

¹⁶⁸ Omar Radi was first arrested in 2019 after he posted a message on X (then Twitter) in which he criticized an appeal court judge for upholding heavy prison sentences against activists from the HIRAK El Rif social justice movement.

¹⁶⁹ Interview in person with Omar Radi, April 2026, France

¹⁷⁰ The wave of peaceful protests that emerged in 2011, known as the 'February 20 Movement', took place in various cities in Morocco and called for social justice and an end to corruption.

¹⁷¹ Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited).

¹⁷² See, for example, articles about Omar Radi on Barlamane.com. Barlamane, *المحرّض على العنف... عمر الراضي* [Omar Radi... Inciter of violence], 2 October 2025, <https://barlamane.com/%D8%B9%D9%85%D8%B1-%D8%A7%D9%84%D8%B1%D8%A7%D8%B6%D9%8A-%D8%A7%D9%84%D9%85%D8%AD%D8%B1%D8%B6-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D8%B9%D9%86%D9%81/> (in Arabic) and Barlamane, Omar Radi décline sa participation au débat #GENZ212 et déclenche une polémique en ligne ("Omar Radi declines his participation in the #GENZ212 debate and triggers an online controversy"), 26 October 2025, <https://barlamane.com/fr/omar-radi-decline-sa-participation-au-debat-genz212-et-declenche-une-polemique-en-ligne/> (in French).

“I think that Moroccan surveillance in Europe, where I am now, is as effective as Moroccan surveillance in Morocco. I know that I am followed everywhere I go, I know that my movements are scrutinized. What they do not have is the same means of coercion – they can only monitor me.”¹⁷³

Omar Radi’s case is emblematic of Morocco’s brutal repression of dissenting voices. The authorities have used virtually all the authoritarian tools at their disposal in an attempt to silence, punish and psychologically destroy him. Nevertheless, from his base in Europe, Omar Radi continues to speak out about human rights and social justice in Morocco.

In August 2026, Omar Radi received a threat notification from Apple informing him of a suspected spyware attack targeted at his iPhone. Threat notifications like this, which Apple has been sending since 2021, are a very strong indication that a device has been targeted with sophisticated ¹⁷⁴ Amnesty International is continuing to investigate this attack campaign.

7.2 LISTENING AND WATCHING EVERYWHERE

“The basis of our job is listening” – *Safir*¹⁷⁵

Listening – to both phone and in person conversations – is the primary tool in the unlawful surveillance of human rights defenders in Morocco. *Safir* refers to the deployment of “physical intrusion operations” as the “marking”¹⁷⁶ stage: “In our jargon, ‘marking’ is when you install a GPS with a listening device in a car, or a camera or a microphone at someone’s home... The Electronics Department do that.”¹⁷⁷

Alongside a range of sophisticated digital and analogue tools, as well as the use of human agents, listening also takes place in collaboration with telecommunications (mobile and internet) providers.

7.2.1 PHONE TAPPING THROUGH TELECOM NETWORKS

Amnesty International spoke to several human rights defenders who believed that their phone calls were being listened to or intercepted because of information they subsequently saw published about them in online smear campaigns against them, or referenced in police interrogations. Ali Salem Tamek is president of the Collective of Sahrawi Human Rights Defenders (CODESA) and lives in Laayoune in Western Sahara.¹⁷⁸ According to

Ali Salem Tamek, the manipulated information about him and CODESA that appears in Morocco’s “defamation media” could only be known from private phone calls. He told Amnesty International: “It’s not possible to have access to this information without some kind of phone tapping. We don’t have the technical knowledge to know how they tap the phones or implant the cameras, but we feel it 24/7.”

Similarly, Mohamed Majaoui, a teacher and human rights activist from Al Hoceima in the Rif region, described this surveillance, which was used during the Hirak El-Rif protest movement between October 2016 and June 2017: “When you make any phone call, you feel like you’re being listened to. We were all aware of that.” He further explained that, during an interrogation at a police station in the city of Casablanca in May 2017, officers showed him reports of his phone calls classified by month: “with my friend, with my wife. It was all monitored – even my personal life.”¹⁷⁹

The DGST’s ability to listen to private phone calls relies on the involvement of at least one telecommunications provider. According to *Safir*, this surveillance work is generally undertaken retroactively and is done systematically, with specific agency employees tasked with listening to calls or sometimes transcribing.

¹⁷³ Interview in person with Omar Radi, April 2026, France

¹⁷⁴ Amnesty International, Apple threat notifications: What they mean and what you can do, 11 April 2024, <https://www.amnesty.org/en/latest/news/2024/04/global-apple-threat-notifications-what-they-mean-and-what-you-can-do/>

¹⁷⁵ Interview with *Safir*

¹⁷⁶ In French, ‘ballisage’

¹⁷⁷ Interview with *Safir*

¹⁷⁸ Front Line Defenders, Ali Salem Tamek – Testimony, 31 October 2022, <https://www.frontlinedefenders.org/en/testimonial/ali-salem-tamek-testimony>

¹⁷⁹ Interview by phone with Mohamed Majaoui, February 2026

Safir explained the process: “First of all, you have to find their number. It’s easy. From our technical side, we can find out the number that you’ve called, it all starts with a database. We have access to everything. It’s not a bought system, it’s developed *par la direction* [by the DGST], internally... The first stage of listening starts here... We can look up anything about anyone at any moment. There are normally two or three engineers, they are coordinators between the DGST and [the telecommunications provider]...¹⁸⁰

Despite the requirement of the Criminal Procedure code, which stipulates that recording or seizure of telephone calls should require judicial authorization,¹⁸¹ according to *Safir* telephone conversations are retained by a telecommunications provider, and are available to the authorities without prior judicial authorization. He explained:

“Because calls, everything, it’s recorded automatically. There’s no need to target your number or listen to you live. It’s already in their base.”¹⁸²

This is supported by documentation related to mass surveillance tools that have been purchased by the Moroccan authorities Verint’s Reliant, which would enable such access, as well as by previously documented cases of the use of Maroc Telecom’s networks to facilitate network injection spyware attacks.

According to *Safir*, phone tapping takes place alongside digital location tracking. The DGST uses a combination of satellite and cellular antenna data, allowing them to map a person’s location over time, even if their device is turned off.

Safir explained: “You have geolocation by GPS, or otherwise by BTS [triangulation by relay antennas].” He describes how agents use an in-house system built on an offline version of Google Earth to visualize location data. “It’s just to visually display where the person is. You use this to convey clearly to the guys [other agents], show them the exact position.”

7.2.2 AUDIO AND VIDEO RECORDING IN PUBLIC AND PRIVATE SPACES

In addition to telephone surveillance, the authorities surreptitiously place microphones and other recording devices in private spaces to capture conversations – a practice referred to in French as *balisage*, or “marking”. This marking is generally carried out by agents of the DGST’s Electronics Department. According to *Safir*: “When someone doesn’t [make a phone] call, we can [still] listen to their conversation with their girlfriend. You see, it’s someone who is with him in the car, that’s the work of the microphones.”

In addition to being surveilled via Pegasus spyware and IMSI catchers, journalist Soulaïman Raïssouni was “marked” and filmed as DGST agents became familiar with his routine. A field operation crew planted trackers in his car, which *Safir* explained is an operation which would typically take between five and 10 minutes. This included a GPS tracker, which would run for approximately 15 to 20 days, as well as a microphone on the steering wheel. The signal was transmitted through encrypted FM radio, meaning that the field officers needed to stay within 3km to 4km of the car to monitor the microphone, moving with the target. *Safir* recalled details of the operation, including that Soulaïman Raïssouni drove a Volkswagen Passat, as well as digits from his number plate.

Omar Radi was also surveilled using these methods. Agents would follow him during his meetings at Les Plages de Nations, north of Rabat, where he was carrying out fieldwork, and also in Casablanca. Omar Radi’s knowledge of digital security meant that he would meet in person for important discussions and switch off his phone, which was a “big problem” for the agents, according to *Safir*: “It was crucial to know what was said during those meetings because what is said between people is more important than the information on the phone”.¹⁸³

To get around the issue of astute targets evading surveillance, *Safir* explained how agents would resort to more traditional, low-tech methods which also required more elaborate preparation. *Safir* recalls: “If I knew he [Omar Radi] was meeting with [human rights defender] Maâti Monjib in a certain café, then I’d talk to the owner and ask him which table he’d sit them at, so we can put microphones and cameras close to it”.¹⁸⁴ The waiter would be bribed to ensure the targets sat at the table where the devices were hidden.

¹⁸⁰ Interview with *Safir*.

¹⁸¹ At least one telecommunications provider operating in Morocco, Orange, has indicated that (as of 2023) Moroccan authorities restrict public disclosure of the number of state requests for interceptions or access to customer data. See, Orange Transparency Report for Freedom of Expression, Information and Respect for Private Life, 2024 Report - Data for the year 2024, p.26, <https://assets.orange.com/medias/domain12751/media101368/410662-tw9bcb6lsx.pdf>

¹⁸² Interview with *Safir*.

¹⁸³ Interview with *Safir*.

¹⁸⁴ Interview with *Safir*.

Omar Radi also told Amnesty International about these café meetings with Maâti Monjib: “Of course I knew there was always the possibility that they’d listen to us or install something. Now I have confirmation. It’s like Kafka.”¹⁸⁵

Even the inside of private homes and spaces do not escape the state’s gaze and can be observed through the use of miniature cameras, often hidden in TVs, air conditioners or other innocuous locations.

Omar Radi’s apartment became such a target. *Safir* explained how miniature microphones, operated wirelessly via encrypted radio transmission, were implanted in his light fixtures – the central and discreet location being an ideal spot. They were so small, some the size of a small coin, that detection was highly unlikely.

Maâti Monjib, who is still based in Morocco, believes that the intelligence services continue to use such forms of surveillance against him as punishment for his human rights work and academic writing. He suspects he is under audio surveillance – most likely from microphones concealed in or near his home. He also turns off his phone while at home, as do associates who visit him there.

Cameras are surreptitiously installed when targets are known – or suspected – to be away from their homes or offices. Public holidays such as Eid al-Kebir are ideal: “The target must be absent, because it takes time,” said *Safir*.

Although miniature cameras are a relatively simple technology, the methodology for hiding such surveillance devices is detailed and specialized. Cameras hidden in walls, for example, can be covered with a plate the same colour as the wall paint, which is actually a one-way transparent screen that becomes imperceptible to most. These operations require the cooperation of several teams and agents. As *Safir* explained:

“We opened the television sets and installed cameras in them. This installation is carried out in a secure environment through team coordination: there is no risk. During the marking stage, people in the field follow [the target]. They don’t let [the target] go. There are always two teams: the one that monitors, the one that installs. Every team has their own job.”¹⁸⁶

In January 2021, veteran human rights activist Fouad Abdelmoumni publicly announced that he and his fiancée were filmed using hidden cameras placed inside his home without his knowledge.¹⁸⁷ The videos had been circulated in 2020 among their contacts on WhatsApp. Fouad Abdelmoumni told Amnesty International:

“When I saw the videos of me and my partner in bed, the location and angle of the recording were clearly visible. It must have been the air-conditioning unit. I went to look but I didn’t find anything, so I deduced that they’d been able to easily install and remove it. The quality of the image and sound was very good, despite the fact it was dark, so the equipment must have been very sophisticated.”¹⁸⁸

Safir told Amnesty International that cameras were indeed hidden in Fouad Abdelmoumni’s home air-conditioning unit. When describing the DGST’s use of miniature cameras hidden in walls and air-conditioning units, he cited the example of Fouad Abdelmoumni as a “textbook case”. Thorough post-surveillance clean-up of hidden surveillance devices is part of a strict protocol. “They’re removed afterwards,” he said. “We leave no trace”.¹⁸⁹

Living with the suspicion of intrusion into the most private and domestic spaces has a profound psychological impact. Kholoud Mokhtari, human rights defender and wife of Soulaïman Raoussouni, told Amnesty International: “I’m not free anywhere. Even at home. My mum says that no one can take a shower in our home. You never know who’s watching.”¹⁹⁰

¹⁸⁵ Interview in person with Omar Radi, April 2026, France.

¹⁸⁶ *Safir* told Amnesty International that teams’ tasks were deliberately kept separate and were carried out without question. In the article ‘Morocco’s Governance of Cities and Borders, AI-Enhanced Surveillance, Facial Recognition, and Human Rights’ the authors write “In the words of an interviewee who did not want to be listed, ‘as a police officer, we do not ask about these things, I guess we do not have the right even, we are simply trained to use new technologies when they are deployed.’” From *The Cambridge Handbook of Facial Recognition in the Modern State*, Chapter 19, pp. 267 - 284, 2024, Cambridge University Press, 267 - 284, 2024, Cambridge University Press, <https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/morocco-governance-of-cities-and-borders/2AB3D0AF6B14CAD564BAD283D5466120>

¹⁸⁷ <https://www.economist.com/middle-east-and-africa/2021/01/28/morocco-regime-is-accused-of-blackmailing-critics>, January 2021 The Economist, “Morocco’s regime is accused of blackmailing critics”, <https://www.economist.com/middle-east-and-africa/2021/01/28/morocco-regime-is-accused-of-blackmailing-critics>, January 2021.

¹⁸⁸ Interview by phone with Fouad Abdelmoumni, December 2025.

¹⁸⁹ Interview with *Safir*.

¹⁹⁰ Interview by phone with Kholoud Mokhtari, December 2025.

Video surveillance continues into public areas. On request from the police or intelligence services, the DGSN can provide access to all state cameras, in public spaces and major streets.

Safir confirmed:

“For public cameras, state cameras, yes, we have access to them... Access is not obtained directly at our level [DGSN]. It is provided by the DGSN.¹⁹¹ They give us what we need. This organization creates a functional pipeline that connects the police operator to the intelligence service, ‘on request’.”

Nor is access limited to state cameras. Private cameras connected to networks can also be accessed. Using a tool called NightHawk, a device the size of a small suitcase produced by Israeli cyber intelligence company Interionet, authorities can access additional cameras, even those unconnected to the internet.

As *Safir* explained:

“Just put it [NightHawk] within 50 metres of a targeted location — and it scans the IP addresses related to the cameras in the perimeter. Even those not connected to the internet. The effectiveness is remarkable. With this system we can locate them, target them remotely. It is a very powerful tool.”

Media outlets, including We Are Tech Africa and government-aligned moroccoworldnews.com, have reported that the Moroccan government is spending millions of dollars on AI-powered facial recognition and behaviour recognition technologies in the run-up to the 2030 World Cup.¹⁹² These technologies have the potential to vastly expand the government’s ability to conduct mass surveillance across the country. It is assumed this will be conducted without judicial authorization, given the patterns of surveillance documented throughout this chapter.

Even in areas where there are no cameras, targets can be followed and recorded from cars or vans specifically designed for covert surveillance. *Safir* explained:

“From the car you see outside, but from outside you see nothing. This technology, which goes beyond tinted windows, uses unidirectional materials that allow complete observation without the risk of detection.”

The practice of surveillance extends to prisons and other official places of confinement. The clandestine installation of microphones and cameras in places of detention is code-named “*Abdessamiaa*”¹⁹³ – literally, “the one who hears everything”.

Safir explained why surveillance against targets is deployed even when they are incarcerated: “We can have influence in prison too. For example, if there are four people in a cell, we want to know what he’s saying, if he wants to get something out, if he’s suicidal, if someone wants to kill him... The operation’s always open.”¹⁹⁴

Since, according to *Safir*, audio material can be more useful than visual material, microphones are the primary form of surveillance in prison. Mobile telephones – although theoretically banned in detention – are tolerated for targets of surveillance precisely to enable agents of the state to listen to private conversations.

CASE STUDY: SOULAIMAN RAISSOUNI

“We must always be careful to reduce the impact of this permanent surveillance, that’s it. Just to reduce ... We can’t eliminate it.”¹⁹⁵

Soulaiman Raissouni is a Moroccan journalist and human rights defender who has been a vocal critic of the authorities for many years. As a result, he became a target for repression, and his case is an

¹⁹¹ The Direction Générale de la Sûreté Nationale, Morocco’s national police force.

¹⁹² We Are Tech, “Morocco to Deploy 4,000 Smart Cameras in Rabat by Year-End”, 24 March 2025, <https://www.wearetech.africa/en/files-uk/news/tech/morocco-to-deploy-4-000-smart-cameras-in-rabat-by-year-end>; Biometric Update, “Facial recognition for Morocco’s Tangier stadium ahead of 2030 World Cup”, 22 October 2025, <https://www.biometricupdate.com/202510/facial-recognition-for-moroccos-tangier-stadium-ahead-of-2030-world-cup>; Morocco World News, “4,000 AI Cameras Coming to Rabat: Security Boost or Privacy Threat?”, 20 March 2025, <https://www.moroccoworldnews.com/2025/03/186146/4000-ai-cameras-coming-to-rabat-security-boost-or-privacy-threat/>; Skyline International, “Morocco’s surveillance infrastructure expands ahead of the Africa Cup and World Cup”, 17 April 2025, <https://skylineforhuman.org/en/news/details/816/moroccos-surveillance-infrastructure-expands-ahead-of-the-africa-cup-and-world-cup>

¹⁹³ In Arabic: عبد السميع

¹⁹⁴ Recording in detention is not prohibited under international human rights law, and is in fact recommended in situations such as interrogation, in order to defend against coercion and ill-treatment. However, where is undertaken outside the law, or for illegitimate aims, such as in this case, targeting HRDs for their lawful exercise of rights, it violates international law and standards. See generally, Amnesty International, Fair Trial Manual, Second Edition, Ch. 9.6, 9 April 2014, POL 30/002/2014.

¹⁹⁵ Interview by phone with Soulaiman Raissouni, December 2025

example of how the authorities employ surveillance in conjunction with smear campaigns against critics, and how this repression can extend to family and networks.

As described in Section 7.2.2, Soulaïman Raïssouni was subjected to both physical and digital surveillance, as were several of his relatives. *Safir* recalled how Soulaïman Raïssouni's personal habits facilitated surveillance, that he was easier to follow because he was "less mobile, maybe because he was married".

This targeting extended to Soulaïman Raïssouni's family. His niece, Hajar Raïssouni, was separately sentenced to one year's imprisonment in 2019, on criminal charges of extra-marital sex and abortion.¹⁹⁶ She reported that during her interrogation she was asked more about her uncle than herself.¹⁹⁷ Hajar Raïssouni's phone number and that of her husband were among the 50,000 potential Pegasus targets shared publicly in 2021 as part of the *Pegasus Project*.¹⁹⁸

In May 2020, allegations that Soulaïman Raïssouni had sexually assaulted a gay man emerged on Facebook. These allegations were amplified and embellished in pro-government media outlets including Chouf TV, Barlamane and Le360.¹⁹⁹

On May 17, Chouf TV published an article online addressing Raïssouni with the title "This is the last warning before your destruction".²⁰⁰

Soulaïman Raïssouni responded by publishing a critical editorial that criticized the actions of the DGSN, the DGST and the Prosecutor's office.²⁰¹

Two days later, on 22 May 2020, he was arrested on charges of indecent assault. Reporters from ChoufTV, a Moroccan website and media outlet known for conducting smear campaigns against human rights defenders and journalists,²⁰² were present in the street at the time of his arrest. They held cameras close to him and filmed the arrest.²⁰³ *Safir* confirmed that, usually, footage or stills from pro-Makhzen, or state-aligned, media outlets will be taken "very close to the scene. If it's [taken] from far away, it's us [recording from a vehicle]".

Soulaïman Raïssouni was held in prolonged solitary confinement during pre-trial detention and in April 2021 undertook a hunger strike, losing 31kg, while being denied medical care. Prison guards searched his cell and seized his personal belongings in retaliation to his hunger strike. They also ramped up the monitoring of his phone calls to his family.²⁰⁴ According to *Safir*, during this time the DGST were working to manufacture evidence of his wife's infidelity that could be shown to him while in prison (see also the case study of Khouloud Mokhtari, below). *Safir* confirms that the purpose was to destroy him, both psychologically and reputationally:

"Imagine Soulaïman Raïssouni in prison and he finds out his wife has been cheating on him. Imagine the reaction of a person who's done everything, who's spoken for and about the people, who loves his wife... It's to break him, you see?"²⁰⁵

¹⁹⁶ Amnesty International, Urgent Action: Morocco: Journalist Detained Over Bogus Charges: Hajar Raïssouni, 13 September 2019, <https://www.amnesty.org/en/documents/mde29/1038/2019/en/>

¹⁹⁷ Amnesty International, "Morocco: Journalist jailed for one year over unlawful abortion in devastating blow for women's rights", 30 September 2019, <https://www.amnesty.org/en/latest/news/2019/09/morocco-journalist-jailed-for-one-year-over-unlawful-abortion-in-devastating-blow-for-womens-rights-2/>; See also, Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited).

¹⁹⁸ Daraj, "The Day Morocco Bugged Us: Hajar Raïssouni's Story", 6 August 2021, <https://daraj.media/en/the-day-morocco-bugged-us/>; Al Jazeera, "From Middle East to India, women 'violated' in Pegasus phone hack", 11 August 2021, <https://www.aljazeera.com/news/2021/8/11/women-pegasus-nso-spyware-scandal-india-middle-east-phone>

¹⁹⁹ Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited).

²⁰⁰ ChoufTV, "Slaimina Raïssouni: This Is the Last Warning before Your Destruction", <https://chouftv.net/press/250314.html>, 17 May 2020

²⁰¹ Facebook post by Soulaïman Raïssouni, <https://www.facebook.com/photo.php?fbid=2722263201390090&set=a.1862560250693727&type=3&theater>, 20 May 2020

²⁰² UN Human Rights Council Working Group on Arbitrary Detention, A/HRC/WGAD/2022/31, July 2022. Point 4.b. states "Several news sites close to the intelligence services, including Chouf TV and Barlamane, which are often involved in the defamation of political opponents and journalists, called for Mr. Raïssouni's arrest"

²⁰³ Chouf TV, 15 أو 4 شوفو شحال ديال البوليس شدو... أول فيديو للحظة اعتقال سليمان الريسوني. ["The first video of the moment of Soulaïman Raïssouni's arrest... Look at Chahal Dial the police pulled him 4 or 15"], 22 May 2020, <https://www.youtube.com/watch?v=fR3jPSSiNOQ> (in Arabic).

²⁰⁴ Amnesty International, Morocco: Critically ill hunger-striking journalist must be granted adequate medical care, 28 May 2021, <https://www.amnesty.org/en/latest/news/2021/05/morocco-critically-ill-hunger-striking-journalist-must-be-granted-adequate-medical-care-2/>

²⁰⁵ Interview with *Safir*.

When, between 2020 and 2022 Soulaïman Raïssouni and Omar Radi were detained in adjacent cells, they passed notes each Sunday. In 2022, guards confiscated their “Sunday letters”, along with the novel Raïssouni had been writing.²⁰⁶

Despite being released by royal pardon in 2024, Soulaïman Raïssouni told Amnesty International that the smear campaign against him continues with ferocity.²⁰⁷ He explained that the content has adopted a different dimension, portraying him as antisemitic,²⁰⁸ and a traitor to his country.²⁰⁹ Soulaïman Raïssouni thinks the strategy is also designed to “cause problems with embassies” and disrupt his chances of being able to move out of the region, as so many other Moroccan human rights defenders have felt forced to do to find safety.

Despite facing such a wide array of tactics in the authorities’ surveillance toolbox, Soulaïman Raïssouni is adamant he will continue speaking truth to power: “The journalistic landscape in Morocco is very bleak. Nearly all of us live in fear. But I won’t stop. I’ll still remain true to myself. Despite these conditions, despite these circumstances, despite everything. Voilà.”²¹⁰

7.3 HUMAN SOURCES

As with listening, the process of watching targets involves a range of techniques – from the most basic to the technically sophisticated – creating a further layer in the near inescapable web of surveillance.

At the simplest level, targets are observed by a network of paid informants, as *Safir* explained: “Taxis, concierges, street vendors... Lots of profiles. You can see them sitting in areas where there are no customers, like guys who sell cigarettes but sit where there are no customers – in fact, they’re indicators, human sensors.”

The human rights defenders interviewed for this report also spoke of this tactic. Omar Radi described how, on occasion, he and his friends would have “false discussions” when out in restaurants or bars: “We invented information because we knew that there were people who were listening to us. And it worked many times. There are even newspapers that wrote things that were said in the bar that were false.”²¹¹

During the 2016-2017 Hirak El-Rif protests, *Safir* explained that the authorities relied on local human knowledge and infiltrators in the form of *mokkads* (local officials) alongside sophisticated surveillance technology. A similar pattern exists in Western Sahara, where surveillance against a target involves a web of informants, family members and friends, but with the addition of police and military checkpoints.²¹² Ali Salem Tamek, president of CODESA, told Amnesty International:

“Almost all members of staff are stopped at checkpoints. The police follow my son to school. Everyone’s involved, the teachers, the doctors. If a doctor hands over a medical report, they’re complicit. If you’re not allowed to register at university, they’re complicit. If the landlord won’t rent you a house, they’re complicit. Everyone is somehow involved in gathering data and handing it over to the intelligence services.”²¹³

²⁰⁶ Amnesty International, Morocco: Denying imprisoned academics and journalists access to read and write violates their right to freedom of expression, 3 May 2023, <https://www.amnesty.org/en/latest/news/2023/05/morocco-denying-imprisoned-academics-and-journalists-access-to-read-and-write-violates-their-right-to-freedom-of-expression/>

²⁰⁷ Interview by phone with Soulaïman Raïssouni, December 2025

²⁰⁸ Barlamane, Soulaïman Raïssouni, de l’hostilité envers la patrie à l’antisémitisme [“Soulaïman Raïssouni, from hostility towards the homeland to anti-Semitism”], 2 April 2025, https://barlamane.com/fr/soulaïman-raïssouni-de-l’hostilité-envers-la-patrie-a-l’antisémitisme/?fbclid=IwY2xjawQX3AVleHRuA2FlbQlxMABicmlkETf2ODNhSDB2aWJDnkpOHFTc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODlwMDg5MgABHmAfpc00DFw93TGb-tNcPFYDluDNkKFCChjxCMQddAcvsUHoDaoKKMZLTy_y_aem_9MKCQaH3-_cThkCqVaaLsQ

²⁰⁹ <https://www.facebook.com/share/p/1DiukvBmWe/?mibextid=wwXlfr>

²¹⁰ Interview by phone with Soulaïman Raïssouni, December 2025

²¹¹ Interview in person with Omar Radi, April 2026, France

²¹² Amnesty International, Morocco must investigate killing of 14-year-old Sahrawi at protest site, October 2010, <https://www.amnesty.org/en/latest/news/2010/10/marruecos-investigar-homicidio-saharaui-14-anos/>

²¹³ Interview by phone with Alisalem Tamek, December 2025

7.4 DIGITAL FORENSIC TOOLS

Mobile forensic tools or mobile data extraction products are specialized systems used by law enforcement or intelligence services to recover, analyse, and interpret data from mobile devices for legal or investigative purposes. While they have legitimate uses as part of law enforcement investigations, they can also be used to bypass device security settings and provide complete access to all data on a device. In 2024, Amnesty International demonstrated how digital forensics products produced by Cellebrite were used as part of a surveillance campaign against Serbian civil society.²¹⁴ Testimony from *Safir* has revealed how the Moroccan authorities used digital forensics tools to access the private data of activists. In order to gain physical access to a device, the authorities use a variety of techniques in various locations, including airports and places of detention.

The operation against Omar Radi illustrates this approach. Less than two weeks after Amnesty International published confirmation of his being targeted with Pegasus spyware, Omar Radi and his fellow journalist Imad Sitou were arrested following an altercation with a cameraman from ChoufTV. At the police station in Casablanca, *Safir* was instructed to access their phones and return them to the journalists. *Safir* recalled that Omar Radi had two devices: an Android phone and a locked iPhone. The latter required Cellebrite's universal forensics extraction device (UFED) in order to access it. The whole operation took around 1 hour and 45 minutes. The Cellebrite device took the extracted data, imported it, and displayed it on a searchable interface.

Omar Radi confirmed he had two phones in his possession on that occasion, both of which were confiscated: "Normally police custody is 48 hours, but they only kept me for 24 hours. I was sure they were going to do something on my phones. So it was Cellebrite they used... Well, congratulations, Messieurs!"²¹⁵

Safir told Amnesty International that Cellebrite's UFED tool was also used on the computer of Taoufik Bouachrine, a Moroccan journalist and human rights defender who has faced speech-based prosecutions, surveillance (including cameras allegedly planted covertly in his office), judicial harassment and harassment campaigns in pro-Makhzen media.²¹⁶ According to *Safir*:

"Colleagues worked on [Taoufik] Bouachrine's phone during the night shift. Cellebrite UFED for Desktop was used on his computer. This is not a box, but a software. Back then the Cellebrite machines were taken to the Rif region. There is a way to do forensics without leaving traces on the device."

CASE STUDY: FOUAD ABDELMOUMNI

"I'd never say in private anything I wouldn't say in court or on TV" – Fouad Abdelmoumni

Fouad Abdelmoumni is a Moroccan economist and veteran human rights activist. Now living in Switzerland, he has been subjected for many years to surveillance and repression by the Moroccan authorities, including through the use of Pegasus spyware, and criminalization for exercising his right to freedom of expression. In 2020, an anonymous WhatsApp account sent intimate videos of Fouad Abdelmoumni and his partner at home to their friends, family and some fellow activists.

According to Fouad Abdelmoumni, prior to the videos being circulated on WhatsApp, pro-Makhzen media outlet ChoufTV threatened to publish them in what he considered an attempt to blackmail him into silence. Sex outside of marriage constitutes a crime in Morocco, punishable with a prison sentence under Article 490 of the Penal Code. It is also particularly stigmatized for women and LGBTI people in Moroccan society, due to the prevalence of heteropatriarchal norms.

Nevertheless, Fouad Abdelmoumni considers himself to be lucky: his partner was prepared to face "the pressure"; his family were accepting of his relationship ("which is rare in Morocco," he said), and his

²¹⁴ Amnesty International, "A Digital Prison": Surveillance and the suppression of civil society in Serbia: Executive Summary" (Index: EUR 70/8814/2024), 16 December 2024, <https://www.amnesty.org/en/documents/eur70/8814/2024/en/>

²¹⁵ Interview in person with Omar Radi, April 2026, France

²¹⁶ Taoufik Bouachrine, publisher of Akhbar el-Youm, one of the country's last opposition newspapers, was sentenced to 15 years in prison for sexual assault against several women. In its opinion about this case, the United Nations' Working Group on Arbitrary Detention concluded that his trial was marred by due-process violations and considered that Bouachrine's detention forms part of a "judicial harassment attributable to nothing other than his investigative journalism." See full summary of Bouachrine's case in: Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited). See also, Amnesty International, "Morocco: Denying imprisoned academics and journalists access to read and write violates their right to freedom of expression", 3 May 2023, <https://www.amnesty.org/en/latest/news/2023/05/morocco-denying-imprisoned-academics-and-journalists-access-to-read-and-write-violates-their-right-to-freedom-of-expression/>; Amnesty International, "Morocco: Journalist targeted by authorities faces trial", 6 April 2021, <https://www.amnesty.org/en/latest/press-release/2021/04/morocco-journalist-targeted-by-authorities-faces-trial/>

socioeconomic status afforded him a level of protection that many do not have. “I’m privileged,” he told Amnesty International. “There are people who suffer so much more and who simply don’t dare to speak about it.”

“I always thought there was a red line that the Moroccan state wouldn’t cross, around the use of intimate information. Yes, it’s certain that they spy on us, that they have recordings, that they use those to blackmail people – but never to put them in the public sphere. And then I saw what they did with [Moroccan journalist] Taoufik Bouachrine.²¹⁷ That was a real shock. When they did that with other people, including me, I knew they’d reached a level of repression we hadn’t seen before.”²¹⁸

The online smear campaigns directed against Fouad Abdelmoumni continued when he moved to Europe. On 28 October 2024, he commented on a friend’s Facebook post criticizing Franco-Moroccan relations and referring to the Moroccan government’s use of Pegasus spyware to target dissidents. Four days later, a Casablanca court charged him with “insulting organized bodies, publishing false allegations, and reporting an imaginary crime that he knows did not occur”.²¹⁹ Fouad Abdelmoumni told Amnesty International that news of the charges were published hours before he was actually charged. On 3 March 2025, he was sentenced in his absence to six months in prison for “spreading false allegations”.²²⁰ Almost 300 human rights defenders and researchers signed a petition calling for the authorities to overturn his conviction.²²¹ At the time of publication of this report, Fouad Abdelmoumni was waiting for a summons for the appeal.

7.5 SURVEILLANCE OPERATIONS

The following case studies describe how different surveillance techniques are used in combination and over time to monitor activists and human rights defenders in areas where there is real or perceived opposition to the government.

These include Western Sahara, where ongoing conflict is one of the most sensitive political topics in the country, and the northern Rif region, where mass protests broke out in 2016 and 2017.

Most of Western Sahara, a non-self-governing territory since 1963,²²² has been under Morocco’s de facto control since it seized the territory from Spain in 1975.²²³ The Moroccan government considers it to be Moroccan territory and rejects demands for a vote on self-determination that would include independence as an option and criminalizes and suppresses any speech that questions Moroccan sovereignty over Western Sahara. The Moroccan government has often prosecuted people for speech related to Western Sahara’s status under provisions that criminalize questioning the “territorial integrity” of Morocco. The authorities have also consistently repressed Sahrawi activism, denying their freedom of expression, assembly and association and often arresting and imprisoning them for that activism.²²⁴

The Hirak El-Rif protests were a sustained protest movement in the Rif region of northern Morocco throughout 2016 and 2017 that demanded an end to the marginalization of their communities and made

²¹⁷ DAWN, “Morocco: Activist Sentenced for Peaceful Speech”, 27 March 2025, <https://dawnmena.org/morocco-activist-sentenced-for-peaceful-speech/>

²¹⁸ Interview by phone with Fouad Abdelmoumni, December 2025.

²¹⁹ Human Rights Watch, “Morocco and Western Sahara: Events of 2024”, <https://www.hrw.org/world-report/2025/country-chapters/morocco-and-western-sahara> (accessed on 30 July 2026).

²²⁰ Human Rights Watch, “Morocco: Activist Sentenced for Peaceful Speech”, 27 March 2025,

<https://www.hrw.org/news/2025/03/27/morocco-activist-sentenced-peaceful-speech>;

Amnesty International, *The State of the World’s Human Rights: April 2026* (Index: POL 10/0320/2026), 21 April 2026,

<https://www.amnesty.org/en/documents/pol10/0320/2026/en/>, p. 260.

²²¹ H24Info, Maroc: une pétition demande l’annulation de la condamnation de Fouad Abdelmoumni [Morocco: Petition calls for annulment of Fouad Abdelmoumni’s conviction], 18 March 2025, <https://h24info.ma/maroc/une-petition-demande-lannulation-de-la-condamnation-de-fouad-abdelmoumni/> (in French); Arab News, “Rights advocates urge Morocco to annul activist’s prison term”, 18 March 2025, <https://www.arabnews.com/node/2593948/middle-east>

²²² UN, The United Nations and Decolonization: Western Sahara, 9 September 2024,

<https://www.un.org/dppa/decolonization/en/hsgt/western-sahara>

²²³ Amnesty International, “Western Sahara: Long-term prisoners await justice”, 8 November 2022,

<https://www.amnesty.org/en/latest/news/2022/11/western-sahara-long-term-prisoners-await-justice/>

²²⁴ This option was included in a referendum that Morocco and the Polisario Front, the liberation movement for Western Sahara, agreed to in a 1991 UN-brokered ceasefire agreement. In October 2025, the UN Security Council adopted a resolution calling for negotiations to achieve self-determination for the people of Western Sahara.

social justice related demands. The authorities responded with hundreds of arrests and prosecutions.²²⁵ The region, whose population is predominantly Amazigh,²²⁶ has a history of rebellion against government control.²²⁷ Its people have faced systemic political, economic and cultural marginalization and widespread repression from the Moroccan authorities.²²⁸

Safir spoke of Sahrawis and Rifians as being priority targets of the Moroccan intelligence services both in Morocco and in Spain.

CASE STUDY: SAHRAWI ACTIVISTS

“In Western Sahara, everyone is under surveillance.”²²⁹

“We’re talking about occupation here, the denial of a sovereign nation. Morocco puts all its efforts in to counter this. The repression is on another level.” – El Mahjoub Maliha

Amnesty International and other civil society organizations²³⁰ have repeatedly documented violations against Sahrawi activists in an attempt to silence or punish them for their peaceful activism.²³¹ For example, in January 2024, police violently dispersed a peaceful demonstration by Sahrawi women activists in Laayoune, Western Sahara’s largest city, and subjected protesters to beatings.²³² In May 2025, eight UN Special Rapporteurs denounced Morocco’s “ongoing campaign of repression, racial discrimination, and violence against Sahrawi human rights defenders, journalists, and advocates for self-determination”.²³³

After winning the Front Line Defenders Award for Human Rights Defenders at Risk in December 2025, Mhamed Hali, a Sahrawi lawyer, told Amnesty International: “As Sahrawi defenders, we are often targets of repressive measures such as arrest, abduction, physical assault, illegal prosecution and defamation of us and our families.”²³⁴ These repressive measures also include both physical and digital surveillance.

Following the Pegasus Project revelations of 2021, Amnesty International’s Security Lab confirmed forensically that the phone of prominent Sahrawi human rights defender Aminatou Haidar had been infected with Pegasus spyware on multiple occasions.²³⁵ Such targeting is not restricted to Sahrawi human rights defenders within the Moroccan/Western Sahara borders. The Pegasus Project also revealed that Sahrawi activist and Belgian citizen El Mahjoub Maliha was targeted and infected with Pegasus spyware while in Belgium. French citizen Claude Mangin,²³⁶ the partner of Naama Asfari, a Sahrawi activist who is imprisoned in Morocco, was also targeted in France. In December 2025, Amnesty International interviewed Ali Salem Tamek,²³⁷ president of Sahrawi human rights organization CODESA, alongside El Mahjoub Maliha, CODESA’s head of external relations. Ali Salem Tamek had been renting a house in Laayoune, the largest city in Western Sahara, and used it as a base for

²²⁵ Amnesty International, “Hirak el Rif appeal must deliver justice after deeply flawed trial,” 17 December 2018,

<https://www.amnesty.org/en/latest/press-release/2018/12/morocco-hirak-el-rif-appeal-must-deliver-justice-after-deeply-flawed-trial/>

²²⁶ The Amazigh people, also known as Berber, are Indigenous Peoples from North Africa, and include the Rifians who inhabit the Rif region of Morocco.

²²⁷ International Committee of the Red Cross (ICRC), *The Rif War: A forgotten war?*, June 2023, International Review of the Red Cross No. 923, <https://international-review.icrc.org/articles/the-rif-war-a-forgotten-war-923> and <https://international-review.icrc.org/articles/the-rif-war-a-forgotten-war-923>; Nabil Mouline, *Reconsidering the Rif Revolt (1958-59)*, 28 January 2015, Maghreb, <https://www.jadaliyya.com/Details/31718>

²²⁸ Ellen Debackere and Yassin Akouh, “Five years of Rifian protests: We see no difference”, 12 November 2021,

<https://carnegieendowment.org/sada/2021/11/five-years-of-rifian-protests-we-see-no-difference?lang=en>;

<https://www.tandfonline.com/doi/abs/10.1080/13629387.2020.1780921>

²²⁹ Interview by phone with Ali Salem Tamek, December 2025.

²³⁰ See, for example, CIVICUS, “Authorities tighten rights clampdown in Western Sahara, youths hold mass protests”, 28 October 2025,

<https://monitor.civicus.org/explore/authorities-tighten-rights-clampdown-in-western-sahara-youths-hold-mass-protests/>

²³¹ Amnesty International, “Morocco/Western Sahara: Targeted Crackdown of Sahrawi Activists”, 19 July 2021

<https://www.amnesty.org/en/documents/mde29/4404/2021/en/>

²³² Amnesty International, *The State of the World’s Human Rights: April 2025*, (Index: POL 10/8515/2025), 28 April 2025,

<https://www.amnesty.org/en/documents/pol10/8515/2025/en/>

²³³ Western Sahara Resource Watch, “UN experts call on Morocco to stop demolishing Saharawi homes”, 2 June 2025,

<https://wsrw.org/en/news/un-experts-call-on-morocco-to-stop-demolishing-saharawi-homes>

²³⁴ Amnesty International, “Mhamed Hali: “Despite the dangers, bringing smiles to the faces of forgotten victims makes it worth continuing””, 9 December 2025, <https://www.amnesty.org/en/latest/campaigns/2025/12/mhamed-halidespite-the-dangers-bringing-smiles-to-the-faces-of-forgotten-victims-makes-it-worth-continuing/>

²³⁵ Amnesty International, “Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence”, 9 March 2022, <https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/>

²³⁶ Amnesty International, Appendix D: Pegasus Forensic Traces per Target, 27 July 2021,

<https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/>

²³⁷ Front Line Defenders, “Ali Salem Tamek – Testimony”, 31 October 2022, <https://www.frontlinedefenders.org/en/testimonial/ali-salem-tamek-testimony>

CODESA: “It’s constantly under surveillance. Whenever we have an event, they block people from entering. The landlord is going to kick me out. I can’t find anyone else who will dare rent me a house”. He was evicted in April 2026.²³⁸

Amnesty International confirmed that, in February 2024, police prevented a press conference on the human rights situation in Western Sahara taking place at Ali Salem Tamek’s home.²³⁹ During 2025, CODESA reported ongoing arbitrary arrests of Sahrawi activists, prolonged surveillance, house arrests of entire families and systematic censorship tactics used against protest organizers.²⁴⁰ They also reported an escalated crackdown on their members between 24 February and 4 July 2025.²⁴¹

Similar to the other human rights defenders interviewed by Amnesty International for this report, Ali Salem Tamek has a deep understanding of the psychology of state surveillance:

“It’s not just to know what we’re doing, it’s to prevent what we’re doing. That’s the primary objective: to create fear so people don’t dare speak out. With physical surveillance, people get scared to speak but with digital surveillance they’re even scared to whisper.”

As *Safir* has confirmed, once a target is identified as a high priority, the authorities will use all tools at their disposal to silence them. Ali Salem Tamek has experienced this multifaceted repression: “They’ve tried so many ways to make me stop my activism, I’ve been imprisoned and defamed. I’ve had offers and so have my friends and family. If they can’t buy you, they’ll try to break you.”

CASE STUDY: THE HIRAK EL-RIF MOVEMENT

“[P]eople will think twice before coming out another time” – Omar Radi

The Hirak El-Rif protests took place in the Rif region of Morocco, in the city of Al Hoceima and surrounding areas, between October 2016 and June 2017. They were ignited when fishmonger Mouhcine Fikri was crushed to death by a rubbish truck as he attempted to recover fish confiscated by the local authorities. The protesters were demanding an end to the marginalization of their Amazigh-speaking communities. Their demands related to social justice, health care, employment, infrastructure and cultural identity.

Some of the protests involved violence and clashes with security officers. Between May and July 2017, security forces arrested hundreds of protesters, including children, journalists and protest leaders. Among them was human rights defender and protest leader Nasser Zefzafi,²⁴² who remains in prison despite global campaigns for his release,²⁴³ and credible allegations that his ‘confessions’ were obtained under torture.²⁴⁴ His unjust treatment at the hands of the authorities sent, and continues to send, a strong signal to Rifians that they would be punished if they tried to speak out. Omar Radi, who has been consistently vocal in his defence of the Rifians’ calls for social justice,²⁴⁵ also spoke about this chilling effect on protest: “When you give 20 years in prison to someone who just went out in the street asking for hospitals and stuff, people will think twice before coming out another time”.²⁴⁶

²³⁸ Interview by phone with Ali Salem Tamek and El Mahjoub Maliha, September 2026

²³⁹ Amnesty International, *The State of the World’s Human Rights: April 2025* (previously cited).

²⁴⁰ Amnesty International, *The State of the World’s Human Rights: Amnesty International annual report April 2026*, 21 April 2026, <https://www.amnesty.org.uk/knowledge-hub/all-resources/annual-report-2026/>, p. 261. See also: Fédération internationale pour les droits humains, Maroc / Sahara occidental : harcèlement, surveillance et restrictions continues à l’encontre des membres du Codesa, 28 February 2025, Maroc / Sahara occidental : harcèlement, surveillance et restrictions continues à l’encontre des membres du Codesa

²⁴¹ On 7 May 2025, three United Nations Special Rapporteurs wrote to the Moroccan authorities expressing their deep concern about acts of intimidation, surveillance, harassment and defamation against Alisalam.

²⁴² MENA Rights Group, “Arbitrary detention of Moroccan political activist Nasser Zefzafi since May 2017”, 18 March 2024, <https://www.menarights.org/en/case/nasser-zefzafi>

²⁴³ See, for example, Amnesty International, “Two decades in prison for speaking out”, <https://www.amnesty.org/en/petition/two-decades-in-prison-for-speaking-out/> (accessed on 30 July 2026) and UN Working Group on Arbitrary Detention (WGAD), *Opinions adopted by the Working Group on Arbitrary Detention at its one hundredth session, 26–30 August 2024*, 25 October 2024, UN Doc. A/HRC/WGAD/2024/43,

<https://documents.un.org/doc/undoc/gen/g24/192/85/pdf/g2419285.pdf?https://documents.un.org/doc/undoc/gen/g24/192/85/pdf/g2419285.pdf> and <https://www.hrw.org/news/2023/08/09/worlds-indigenous-peoples-day-ngos-renew-call-release-nasser-zefzafi-detention> and Human Rights Watch, “On World’s Indigenous Peoples Day, NGOs Renew Call for Release of Nasser Zefzafi from Detention in Morocco”, 9 August 2023, <https://www.hrw.org/news/2023/08/09/worlds-indigenous-peoples-day-ngos-renew-call-release-nasser-zefzafi-detention>

²⁴⁴ Human Rights Watch, “Morocco and Western Sahara: Events of 2024” (previously cited).

²⁴⁵ Human Rights Watch, “*They’ll Get You No Matter What*”: Morocco’s Playbook to Crush Dissent (previously cited).

²⁴⁶ Interview in person with Amnesty International, April 2026, France.

Nasser Zefzafi's previous lawyer and former Minister for Human Rights, Mohamed Ziane,²⁴⁷ also remains in prison at the age of 83. He was arrested in November 2022 under bogus charges stemming from his work defending activists, journalists and victims of human rights abuses.²⁴⁸ Mohamed Ziane's file was, according to *Safir*, "hyper-sensitive, ultra secret". *Safir* confirmed that the Research Unit²⁴⁹ was responsible for the files of Nasser Zefzafi and Mohamed Ziane. Other prominent Moroccan human rights defenders who spoke up for the Hirak El-Rif protesters also faced repercussions from the authorities, including surveillance via highly invasive spyware. Lawyer Abdessadak El Bouchattaoui was a part of the legal defence team for the imprisoned protesters. In February 2017, he was sentenced to 20 months in prison for online posts in which he criticized the authorities' use of excessive force during the protests.²⁵⁰ In 2019, Amnesty International's Security Lab confirmed that his device had been targeted repeatedly with malicious SMS messages that carried links to websites connected to NSO Group's Pegasus spyware.²⁵¹

As of the time of publication of this report, seven activists remain in prison for their role in the Hirak El-Rif protest movement of 2017: Nabil Ahmijk, Zakaria Adahchour, Mohamed Haji, Samir Ighid, Mohamed Jelloul, Salah Lachkam and Nasser Zefzafi.

CASE STUDY: AL HOCEIMA, A SURVEILLANCE LABORATORY

"Even little things you forget, they knew about." - Mohamed Majaoui

Mohamed Majaoui is a teacher, activist and president of the Al Hoceima section of the Moroccan Association of Human Rights in the Rif region. He was sentenced to five years in prison for his role in the Hirak El-Rif protests in 2017. When he refused to sign a written statement, which included falsified details incriminating Nasser Zefzafi (see case study above), a police agent threatened to rape his wife and his young daughters.²⁵² He told Amnesty International of the moment the true extent of the surveillance became clear to him after his arrest, when he was held for eight days in a Casablanca police station.

"It was then we realized we were being surveilled every single minute. Everything we did, every meeting we had, every house we went to, when my wife went to visit her mother. Even little things you forget, they knew about." ²⁵³

The surveillance continued after his release from prison under a royal pardon in 2020. Of the 15 Hirak El-Rif activists released from prison with Mohamed Majaoui under the pardon, just four have remained in the country.

Safir's testimony confirms the significant resources dedicated to infiltrating and quashing the Hirak El-Rif movement, noting its "historic" and "political" importance. Speaking to Amnesty International, *Safir* said: "the whole of the DGST was working on El-Rif at that time. Everyone was in El Hoceima. IMSI catchers, wi-fi, spyware – we used everything".²⁵⁴

Authoritarian methods of silencing dissent are more visible and brutal in times of protest²⁵⁵. But, as Mohamed Majaoui, president of the Al Hoceima section of the Moroccan Association of Human Rights,

²⁴⁷ Amnesty International, "Morocco: Human rights lawyer sentenced in absentia: Mohamed Ziane", 31 January 2023, <https://www.amnesty.org/en/documents/mde29/6397/2023/en/>

²⁴⁸ Amnesty International, "Morocco: Human rights lawyer sentenced in absentia: Mohamed Ziane" (previously cited).

²⁴⁹ 'cellule de recherche', which sits under the DOP (Directorate of operations, "Direction des Opérations), within the DGST

²⁵⁰ Amnesty International, "Morocco: Conviction of Hirak human rights lawyer sets a dangerous precedent" 19 February 2018, <https://www.amnesty.org/en/documents/mde29/7912/2018/en/>

²⁵¹ Amnesty International, "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware", 10 October 2019, <https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/>

²⁵² Human Rights Watch, "Morocco: Torture Suspicions Mar Mass Trial Verdicts", 30 November 2018, <https://www.hrw.org/news/2018/11/30/morocco-torture-suspicions-mar-mass-trial-verdicts>

²⁵³ Interview by phone with Mohamed Majaoui, February 2026.

²⁵⁴ Interview with *Safir*.

²⁵⁵ Chantal E. Berman, "Policing the organizational threat in Morocco: Protest and public violence in liberal autocracies", 15 December 2020, *American Journal of Political Science*, Volume 65, Issue 3, <https://onlinelibrary.wiley.com/doi/10.1111/ajps.12565>, pp. 733–754.

explains, they are omnipresent: “The repression [in the Rif] is historic. There’s always been surveillance here. They’re always spying on us.”

DRAFT

8. SMEAR CAMPAIGNS

Human rights defenders and dissenting voices in Morocco often find themselves subject to apparently coordinated smear campaigns alongside surveillance and judicial harassment or criminal prosecution. Human rights defenders have consistently reported to Amnesty International examples of how information that appears in these smear campaigns can only have been obtained via surveillance. The purpose of these smear campaigns is usually to delegitimize them or to stigmatize them in the eyes of Moroccan society.

The role of smear campaigns by state actors and state-aligned private actors is a well-documented threat to human rights defenders around the world. As the UN Special Rapporteur on freedom of peaceful assembly and of association, Gina Romero, has noted:

“Stigmatizing and harmful narratives generated and spread by both State and non-State actors undermine the essence of the rights to freedom of peaceful assembly and of association, leading to serious human rights violations, impunity, closing of civic space, erosion of human rights, polarization and undermining of democracy.”²⁵⁶

She has further noted that:

“Mental health is impacted by multiple additional factors routinely experienced by civil society, including constant targeting ‘by smear campaigns day in and day out. It drains you mentally, physically and socially if you are monitored online, offline, around the clock’, which has led many to leave activism.”²⁵⁷

The experiences of Moroccan human rights defenders bear this out. Indeed, the phenomenon is so commonplace that media outlets known for carrying out such smear campaigns are colloquially known as the “defamation media”. The ideological alignment of several prominent Moroccan media outlets, such as Chouf TV, Barlamane, and Le360 – as well as the alleged links between their leadership and the authorities – has been documented at length by other civil society groups.²⁵⁸ The degree to which the “defamation media” is at the behest of, or merely in close political alignment with, state authorities is impossible to determine in every case, but what is clear is that there are phases where smear campaigns are so intense, widespread and sustained that they contribute significantly to the chilling effect on expression in Morocco.

This phenomenon has also been the subject of denunciation in a manifesto by journalists against the pro-Makhzen “defamation media”,²⁵⁹ and has been widely criticized by Moroccan journalists and activists.²⁶⁰ Human rights defenders and journalists are not the only victims; political opponents have faced the same treatment, including for example the lawyer and former Human Rights Minister, Mohamed Ziane. In 2020, he was subjected to a smear campaign by ChoufTV, which published photos²⁶¹ and what they claimed was

²⁵⁶ Report of the UN Special Rapporteur on Freedom of Peaceful Assembly and of Association, Protecting the rights to freedom of peaceful assembly and of association from stigmatization, UN Doc. A/79/263, 31 July 2024, para. 114.

²⁵⁷ Report of the UN Special Rapporteur on Freedom of Peaceful Assembly and of Association, Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, UN Doc. A/HRC/62/45, 21 April 2026, para. 96.

²⁵⁸ Human Rights Watch, “They’ll Get You No Matter What”: Morocco’s Playbook to Crush Dissent (previously cited), pp. 125-133.

²⁵⁹ En toutes lettres, “Manifeste: Des journalistes marocains contre les médias de diffamation” [“Manifesto: Moroccan Journalists Against Defamatory Media”], 16 July 2020, <https://etlettres.com/manifeste-des-journalistes-marocains-contre-les-medias-de-diffamation/> (in French).

²⁶⁰ See, for example, Reporters Without Borders, “Morocco: one year after royal pardon, press still under attack”, 30 July 2025, <https://rsf.org/en/morocco-one-year-after-royal-pardon-press-still-under-attack> and Abdellatif el-Hamamouchi, “Smear Campaigns and Extortions: Weapons to Silence Opposition in Morocco”, 9 February 2021, smex.org/smeas-campaigns-and-extortions-weapons-to-silence-opposition-in-morocco/

²⁶¹ Chouf TV, “Bouch el-Intemaa: Tafassil Bouch el-Nasr Bighararat w Talaat al-Quran fi Beit al-Rais al-Jazairi” [“Revelation of Belonging: Details of the Victory Revelation with Songs and the Recitation of the Qur’an in the House of the Algerian President”], 15 November 2020, <https://mobile.chouftv.ma/press/315782.html> (in Arabic).

an intimate video²⁶² of him with a client and former police officer Ouahiba Khourchech.²⁶³ According to Khourchech, the photos were taken over more than a year, indicating long-standing surveillance of her and Mohamed Ziane.²⁶⁴ After Mohamed Ziane publicly criticized the director of the Moroccan national security forces in reaction to the defamatory video,²⁶⁵ the Ministry of Interior filed a complaint against him.²⁶⁶

MAKHZEN

Literally meaning 'warehouse', *Makhzen* is a term which predates the colonial era²⁶⁷ and is used to refer to the governing apparatus of Morocco, which includes the security services. Today, Makhzen is not an official entity²⁶⁸ but a complex system of state, social and symbolic power centred around the Royal Palace of King Mohammed VI. Several journalists to whom Amnesty International spoke for this report translated Makhzen as 'deep state'. 'Pro-Makhzen' state-affiliated news websites²⁶⁹ that have been flagged as participating in or carrying out smear campaigns against journalists and human rights defenders featured in this report include Barlamane.com, Le360, and ChoufTV.

Maâti Monjib shared a Moroccan saying which sums up the chilling effect imposed as a result of state repression: "hit the big ones, and the little ones will be afraid."²⁷⁰ Defamation and/or harassment via certain state-aligned media outlets and individuals targeting "the big ones" contributes significantly to this fear.

Maâti Monjib, referred to by Hicham Mansouri as "the most defamed man in Morocco", knows all too well how smear campaigns are deployed. In 2015, Maâti Monjib filed a complaint before the Paris Regional Court (Tribunal de Grande Instance (TGI)) against the Le360 outlet over several defamatory articles. The case was closed in 2017 due to an apparent lack of cooperation from Morocco.²⁷¹ Maâti Monjib's lawyer Patrick Baudouin, former president of the International Federation for Human Rights (FIDH) spoke out against the frustrating judicial process and the use of defamation as a tool of repression in Morocco: "Everyone knows that it [the "defamation media"] reproduces the government's desire to denigrate a certain number of opponents."²⁷²

Despite receiving a royal pardon in July 2024, Maâti Monjib told Amnesty International that he is still subjected to public smear campaigns. For example, on 7 April 2025, a video was published on YouTube which purports to show him in a bar with a romantic partner.²⁷³ Maâti Monjib explained to Amnesty International that the woman was in fact a professor and colleague who teaches in Rabat.

"This was to punish me for my three-day hunger strike, which was in protest at being forbidden to leave the country to attend a conference at the Sorbonne University in Paris," he said.²⁷⁴

The presenter in the YouTube video, whose channel has more than 485,000 subscribers, claims that Maâti Monjib is lying about his hunger strike, and that he was in fact with this woman "smoking shisha and drinking alcohol" at the time. Maâti Monjib believes the video was actually taken at the end of 2024 in Salé. He says that this is one of several incidents of him having been filmed in restaurants or cafes, with claims that he is drinking alcohol and "cavorting with mistresses" in an attempt to discredit him.

Fouad Abdelmoumni told Amnesty International that the smear campaigns against him and his close circle of activists continue to this day: "We're a group of about 10 people, and not a day goes by without defamatory articles targeting us. Not a single day. They can fabricate crimes, accuse us of heinous

²⁶² MENA Rights Group, "Moroccan human rights lawyer Mohammed Zian sentenced to three years in prison", 22 December 2022, <https://menarights.org/en/case/mohammed-zian>

²⁶³ SMEX, "Smear Campaigns and Extortions: Weapons to Silence Opposition in Morocco", 9 February 2021, <https://smex.org/smear-campaigns-and-extortions-weapons-to-silence-opposition-in-morocco/>

²⁶⁴ Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited). <https://www.aljazeera.com/news/2022/11/22/morocco-arrests-former-human-rights-minister>

²⁶⁵ <https://www.morocoworldnews.com/2021/01/62968/moroccos-interior-ministry-files-complaint-against-lawyer-mohamed-ziane/>

²⁶⁶ Judith Scheele, "Northwest African perspectives on the concept of the state", HAU: Journal of Ethnographic Theory, 2022, Volume 12, Number 3, <https://www.journals.uchicago.edu/doi/full/10.1086/722386#r17>

²⁶⁷ Human Rights Watch, "They'll Get You No Matter What": Morocco's Playbook to Crush Dissent (previously cited).

²⁶⁸ Freedom House, "Freedom on the net 2024: Morocco, 2024", <https://freedomhouse.org/country/morocco/freedom-net/2024>

²⁷⁰ Orient XXI, Maâti Monjib. « La corruption est partout au Maroc », 7 April 2025, <https://www.youtube.com/watch?v=yBSlvQEuxyl> (in Arabic). <https://orientxxi.info/Maati-monjib-la-corruption-est-partout-au-maroc.8141> (in French).

²⁷¹ Interview by phone with Maâti Monjib, July 2026

²⁷² Mediapart, P. Baudouin: "Les pratiques du régime de Mohammed VI ressemblent à celles de Ben Ali" [P. Baudouin: "The practices of Mohammed VI's regime resemble those of Ben Ali"], 13 October 2017, <https://blogs.mediapart.fr/hicham-mansouri/blog/131017/p-baudouin-les-pratiques-du-regime-de-mohammed-vi-ressemblent-elles-de-ben-ali> (in French).

²⁷³ Radia Style, منجيب المعطي فضيحة !! أم وغدا خمر اليوم الشيشة بمقهى حميمة جلسة يوثق فيديو [The Muti Manjib Scandal !! Video Captures an Intimate Moment at a Shisha Café, Today: Alcohol or Lunch?], 7 April 2025, <https://www.youtube.com/watch?v=yBSlvQEuxyl> (in Arabic).

²⁷⁴ Orient XXI, Maâti Monjib. « La corruption est partout au Maroc » [Maâti Monjib: "Corruption is rife in Morocco"], (previously cited).

behaviour. They can dredge up things from our personal history, or the history of our friends, relatives and families. There are so many possibilities.”²⁷⁵

Omar Radi too spoke of the incessant monitoring of his activities, online and offline, by the “defamation media”: “As soon as I speak in public, as soon as I write a Facebook post, as soon as I put something out on Instagram, they scrutinize my every move, they insult me. They’re not media – they’re tools of terror”.²⁷⁶ According to Omar Radi, ChoufTV has portrayed him as a “spy”²⁷⁷, traitor²⁷⁸, as well as someone who regularly consumes alcohol, hashish, and [psychotropic drug] Karkoubi.²⁷⁹ Indeed, according to *Safir*, “Omar Radi suffered the most violent campaigns”.²⁸⁰

Maâti Monjib noted that “defamation based on surveillance seems to be more discouraging for the bulk of activists than physical repression... Defamation can lead people to become defamers themselves – due to the pressure. There are many such cases in Morocco, involving journalists who were once critical of the regime”.

Fouad Abdelmoumni spoke of the psychological impact that defamation and media harassment can have on its targets: “I have family and friends who value resistance to repression. However, I’ve seen many people overwhelmed, paralyzed, disoriented, defeated or deeply depressed by what they had endured or feared they would endure [from smear campaigns].” Kholoud Mokhtari told Amnesty International that she spent time at a mental health facility due to the psychological distress caused by what she described as “this lethal media machine”.²⁸¹

Fouad Abdelmoumni also described the disproportionate impact that ‘revelations’ (regardless of their veracity) from surveillance appearing in the defamation media can have on women and LGBTI people.

“Being filmed with my partner when we were not married was a big part of the pressure inflicted on me. In Morocco, if you’re a woman, let alone if you’re gay, this can lead to actual physical harm, not just moral and social harm.”²⁸²

As noted in Chapter 7, this is exacerbated by existing heteropatriarchal and cultural norms and legal restrictions in Morocco, and illustrates how smear campaigns can work together with judicial harassment and repression. As *Safir* noted regarding the criminal prohibition under Moroccan law of consensual extra-marital sex: “[this law] isn’t for kids sleeping everywhere. It’s for those who challenge the state.”

Trumped-up sexual assault charges and “fabricated morality cases”²⁸³ – none of which involve recognized crimes under international law – have also been used as a state tool to punish journalists and human rights defenders, with the aim of “dampening public support for the accused”²⁸⁴ and silencing them. Reporters Without Borders has urged the UN to take a stand publicly against the misuse of “sex charges” against journalists by the Moroccan authorities.²⁸⁵ It is vital for all sexual assault allegations to be properly investigated and for perpetrators of such assaults to be brought to justice, but justice cannot be secured without adequate fair trial procedures. Furthermore, as Moroccan feminist collective Khmissa has stated, the instrumentalization of women in legal cases against independent journalists can impede women’s attempts to seek justice.²⁸⁶

In January 2023, the European Parliament adopted a resolution on the situation of journalists in Morocco (notably the case of Omar Radi). The resolution expressed concerns about freedom of expression, media freedom, surveillance of journalists, the unfair trial and detention of journalists, political prisoners and

²⁷⁵ Interview by phone with Fouad Abdelmoumni, December 2025

²⁷⁶ Interview in person with Omar Radi, April 2026, France

²⁷⁷ Chouf TV, “الجاسوس عمر الراضي كان سكران وخارج من الخمار واعتدى على كاميرامان شوف تيفي [“The spy Omar Radi was drunk and came out of the bar and assaulted the camera of Chouf TV”], 6 July 2020, <https://m.chouftv.net/program/267577.html> (in Arabic).

²⁷⁸ Chouf TV, “النكزة العالمية لعمر الراضي، شهودها، سرها و علاقتها بملف التجسس [“Omar Radi’s ‘Global Sugar’, Her Witnesses, Her Secret and Her Relationship to the Spy File”], 7 July 2020, <https://m.chouftv.net/press/268241.html> (in Arabic).

²⁷⁹ Chouf TV, “قضية عمر الراضي: تجسس وجنس و ردود مرتبكة للطاير الخامس/همسة خاصة لفتيحة أعرور [“The Case of Omar Radi: Espionage, Sex and Confused Responses to the Fifth Column / A Special Whisper by Fatiha Arour”], 2 August 2020, <https://m.chouftv.net/press/277609.html> (in Arabic).

²⁸⁰ Interview with *Safir*

²⁸¹ Interview by phone with Kholoud Mokhtari, May 2026

²⁸² Fouad Abdelmoumni added “A woman who has sexual relations outside marriage or a man who has homosexual relationships can be ostracised, rejected by their family, and often subjected to insults and violence in the home or in public spaces”, Interview with Amnesty International, May 2026.

²⁸³ Reporters Without Borders, Morocco/Western Sahara overview, 2025, <https://rsf.org/en/country/morocco-western-sahara#:~:text=image%20of%20women-.Safety,stepped%20up%20prosecutions%20against%20journalists>.

²⁸⁴ Committee To Protect Journalists, “Morocco’s new tactic to punish journalists: charge them with sex crimes”, 18 March 2021, <https://cpj.org/2021/03/moroccos-new-tactic-punish-journalists-charge-sex-crimes/>

²⁸⁵ ds

²⁸⁶ Khmissa NGO, statement posted on X @khmissa5, 2 September 2020, <https://x.com/khmissa5/status/1301246528498135043>

peaceful protesters, and the “misuse of allegations of sexual assault to deter journalists from performing their duties”.²⁸⁷

CASE STUDY: KHOLOUD MOKHTARI

“Click, view, finish” – *Safir*, discussing the surveillance of Kholoud Mokhtari’s device.²⁸⁸

Kholoud Mokhtari is a Moroccan screenwriter and human rights activist. She is married to journalist Soulaïman Raïssouni, with whom she has two young children. As a woman linked to one of the authorities’ primary targets, she has faced a brutal and particular form of violation. She has been subjected to surveillance, both inside and outside of Morocco, harassment, and defamation in the press.

Kholoud Mokhtari has been a vocal supporter of her husband and critic of the authorities, and believes her public activism²⁸⁹ has led to more intense harassment: “The moment I decided to stand up for myself, I knew they’d do something,” she told Amnesty International.²⁹⁰

Safir said Kholoud Mokhtari’s phone was “always being tapped”. She became a separate target herself. There appear to have been three objectives behind this. The first was to dismantle her reputation, particularly on the grounds of morality linked to patriarchal notions of what it means to be a woman, wife and mother in Morocco. In this way, certain state-aligned media outlets and individuals on social media appear to portray her as a bad mother,²⁹¹ “a prostitute”,²⁹² and as being unfaithful to her husband. “They always say I have a lover. Several lovers,” she said.

The second objective was to break her spirit and destroy her psychologically. The third was to lure her into betraying her husband. *Safir* confirms this. The aim was to show her incarcerated husband, Soulieman Raïssouni, a video of his wife with another man. According to *Safir*, DGST operatives sought to cultivate relationships with Kholoud Mokhtari. Several well-dressed men, referred to by *Safir* as “*les honorables correspondants*”, were sent by the DGST to seduce her.

All three objectives carry one ultimate goal: to harass and silence Soulaïman Raïssouni. In this way, the harm inflicted on Kholoud Mokhtari can be viewed as collateral damage in the authorities’ repressive machinery against their key targets. For Kholoud Mokhtari, this damage cannot be overstated. She described the sustained harassment and surveillance she has experienced as “psychological torture”. Her experience illustrates how fundamental the psychological angle is to repression in Morocco.

As the case of Kholoud Mokhtari illustrates, smear campaigns are a core part of the attack on voices of dissent that includes unlawful surveillance and judicial harassment. This phenomenon is not limited to Morocco and is a well-known threat to human rights defenders globally. As the UN Special Rapporteur on freedom of assembly and of association has noted: “Stigmatization efforts deplete the capacity to organize and mobilize. Surveillance serves a dual function: it gathers information to fuel initial stigmatization and then uses the stigmatized status to justify further surveillance. Tactics include leaking private information collected through illegal surveillance – including the monitoring of intimate domestic spaces – to threaten and discredit activists through smear campaigns.”²⁹³

²⁸⁷ European Parliament Resolution of 19 January 2023 on the situation of journalists in Morocco, notably the case of Omar Radi (2023/2506(RSP)), paras D 1-3, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023IP0014#:~:text=whereas%20in%202020%20Reporters%20Without.3>.

²⁸⁸ Interview with *Safir*.

²⁸⁹ Alkarama, “Maroc : Les représailles subies par la militante Kholoud Mokhtari, portées à l’attention des mécanismes de l’ONU” [“Morocco: Reprisals Against Activist Kholoud Mokhtari Brought to the Attention of UN Mechanisms”], 16 February 2026, <https://www.alkarama.org/fr/articles/maroc-les-represailles-subies-par-la-militante-kholoud-mokhtari-portees-lattention-des> (in French).

²⁹⁰ Interview by phone with Kholoud Mokhtari, December 2025

²⁹¹ Maroc Médias, “حرم سليمان الريسوني.. دخل السجن وترك وراءه زوجة تتسكع في الحانات ثم تدعى القذف في عِرضها من طرف الصحافة الوطنية” [“Soulaïman Raïssouni’s wife... He went to prison and left behind a wife who frequents bars and then claims to have been slandered by the national press”], 30 March 2023, <https://www.marocmedias.com/85956/%D8%AD%D8%B1%D9%85-%D8%B3%D9%84%D9%8A%D9%85%D8%A7%D9%86-%D8%A7%D9%84%D8%B1%D9%8A%D8%B3%D9%88%D9%86%D9%8A-%D8%AF%D8%AE%D9%84-%D8%A7%D9%84%D8%B3%D8%AC%D9%86-%D9%88%D8%AA%D8%B1%D9%83-%D9%88%D8%B1%D8%A7/> (in Arabic).

²⁹² Bladi, “Moroccan Journalist’s Wife Speaks Out: Press Freedom Under Fire in High-Profile Cases”, 10 April 2023, <https://en.bladi.net/moroccan-journalist-wife-speaks-out-press-freedom-under-fire-high-profile-cases.101376.html>

²⁹³ Report of the UN Special Rapporteur on Freedom of Peaceful Assembly and of Association, Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, A/HRC/62/45, 21 April 2026, para. 65.

Human rights defenders interviewed for this report repeatedly described how video and audio gathered during surveillance is used as material for smear campaigns, bribery and blackmail, timed to inflict maximum reputational damage. *Safir* confirmed this tactic, which he referred to as “info-shock”:

“When they are going to arrest someone and then there is a postponement for two months, you will see that, during this period, there will be propaganda media.”²⁹⁴

Soulieman Raissouni told Amnesty International:

“There are friends, colleagues in the Netherlands and Belgium, who have invited me privately to take part in activities there. And that’s appeared in articles. So I know they’re surveilling my emails and instant messages and turning them into ‘journalistic’ material against me”.²⁹⁵

As documented elsewhere in this report, other human rights defenders, including Ali Salem Tamek, Omar Radi, Fouad Abdelmoumni and Maâti Monjib, told Amnesty International that material which could only have been gained from surveillance appeared in pro-Makhzen media.

Human rights defenders further noted that the timing of some smear campaigns aligned with instances of judicial harassment, which reinforced their belief that there was state involvement. As Omar Radi told Amnesty International “They [the “defamation media”] even predict my next arrest.”²⁹⁶

8.1 DEFAMATION VIA SOCIAL MEDIA

Social media platforms are also used to run smear campaigns, influence public opinion and control the narrative around news topics and human rights defenders. This phenomenon has become so widespread that Moroccan civil society refers to the perpetrators as “the electronic flies” or “E-flies” (in Arabic: الذباب الإلكتروني).²⁹⁷ These “electronic flies” are accounts with fake profile pictures which operate in a coordinated manner. They attack the public profiles of Moroccan human rights defenders, and pages in support of them, by posting comments with accusations and insults supporting the narrative of the authorities. For example, following the publication of a report detailing the hacking of Omar Radi’s phone with Pegasus spyware, Amnesty International documented multiple smear campaigns against him on Facebook. In October 2020, Amnesty International notified Facebook of several accounts participating in this kind of activity, and shared multiple examples of campaigns that showed coordination in the attacks against Omar Radi and his supporters.

Meta’s 2021 *Facebook Coordinated Inauthentic Behaviour* report stated that it had:

“removed 385 Facebook accounts, 6 Pages, and 40 Instagram accounts that originated primarily in Morocco and targeted domestic audiences. We found this network after reviewing information about a small portion of this activity in the region shared by Amnesty International.”²⁹⁸

Meta’s report further stated that the people behind this network used fake accounts to criticize “human rights organizations and dissidents” and to “comment on news and pro-government stories from various news outlets including ChoufTV”.²⁹⁹

In 2022, in response to an investigation by the Atlantic Council’s Digital Forensic Research Lab (DFR Lab), Meta removed an additional 43 Facebook accounts. According to the DFR Lab, this was linked to accounts taken down in response to Amnesty International’s research in 2021, and was part of Meta’s efforts to “prevent recidivism by networks previously de-platformed [...] strongly suggesting the two networks were

²⁹⁴ Interview with *Safir*.

²⁹⁵ Interview by phone with Soulieman Raissouni, December 2025.

²⁹⁶ Interview in person with Omar Radi, May 2026, France.

²⁹⁷ SMEX, “Swarms of E-flies Terrorize Human Rights Defenders in Morocco”, 22 February 2022, <https://smex.org/swarms-of-e-flies-terrorize-human-rights-defenders-in-morocco/>

²⁹⁸ Facebook, “February 2021 CIB Report”, February 2021, <https://about.fb.com/wp-content/uploads/2021/03/February-2021-CIB-Report.pdf>

²⁹⁹ Facebook, “February 2021 CIB Report”, February 2021, <https://about.fb.com/wp-content/uploads/2021/03/February-2021-CIB-Report.pdf>

connected.³⁰⁰ According to Google's 2025 *Transparency Report*, Moroccan court orders were issued to request the removal of 10 pieces of online content in 2024, all of which involved allegations of defamation.³⁰¹

The majority of the human rights defenders interviewed by Amnesty International report that they continue to be the subject of defamatory, denigratory or scandalous articles and posts from media outlets and on social media.³⁰² Oral testimony from *Safir* described how the authorities support, and in some cases appear to orchestrate, incidents or events which can be used to fuel social media attacks, which he referred to as 'character assassination'. *Safir* points to the example of Soulaïman Raïssouni's arrest in May 2020 in the presence of ChoufTV reporters (see Case Study: Soulaïman Raïssouni). "It is to destroy them morally, psychologically [...]" added *Safir*. In 2022, the UN Human Rights Council's working group on arbitrary detention noted that "news sites close to the intelligence services, including Chouf TV and Barlamane, which are often involved in the defamation of political opponents and journalists, called for Mr. Raïssouni's arrest [in 2020]".³⁰³

While it is not possible to ascertain in every instance the degree to which such campaigns may be the result of direct state support, or merely align with the interests of the state, the timing, targets and messaging of such campaigns, as well as repeated documented cases of coordinated inauthentic behaviour on Facebook, lead many human rights defenders to suspect direct state support in at least some instances. Indeed, according to *Safir*, paid commenters within the DGST respond to critical news articles online. He described witnessing two large rooms staffed with approximately 150 employees tasked with monitoring the news, writing pro-Makhzen (and anti-human rights defender) comments, and spreading this content online. *Safir* added that some specialist multilingual agents use VPNs (virtual private networks) to intervene on forums outside of Morocco, in English, Mandarin, French and Spanish. "Everyone has their role. There are those who write the comments, those who monitor the news, those who follow Facebook...", he explained.³⁰⁴

8.2 SMEAR CAMPAIGNS AND INTERNATIONAL HUMAN RIGHTS LAW

The experiences of human rights defenders and the testimony of *Safir* illustrate how smear campaigns form a crucial part of a strategy to silence dissent.

While direct state support for such campaigns, such as through sharing of surveillance data or support for online commenters would clearly violate Morocco's obligation to respect the human rights of human rights defenders, Morocco's obligations under international human rights law go further than this. The state must also take steps to protect human rights defenders from smear campaigns by private actors, and fulfil the rights of human rights defenders by creating a safe and enabling environment in which they can carry out their work.³⁰⁵

Indeed, during its most recent Universal Periodic Review cycle at the UN Human Rights Council, Morocco supported several recommendations to do just this, including to "[e]nsure a safe and enabling environment for civil society, as well as freedom of expression, peaceful assembly and association" and to "[t]ake measures to foster a safe, respectful and enabling environment for civil society, human rights defenders and journalists."³⁰⁶

³⁰⁰ Atlantic Council Digital Forensics Lab, "How inauthentic Facebook accounts targeted detained Moroccan journalists", 17 November 2022, <https://medium.com/dfrlab/how-inauthentic-facebook-accounts-targeted-detained-moroccan-journalists-fef53534bada>

³⁰¹ Google Transparency Report, https://transparencyreport.google.com/government-removals/government-requests/MA?hl=en&lu=country_request_amount&country_item_amount=group_by:requestors&country_request_amount=group_by:reason_s (accessed on 30 July 2026).

³⁰² Fouad Abdelmoumni, Maâti Monjib, Omar Radi, Afaf Bernani, Soulaïman Raïssouni, Kholoud Mokhtari. For example, within hours of an article written by Omar Radi for Orient XXI about Gen Z appearing online on 28 April 2026, several defamatory AI-generated cartoons had been generated and shared online.

³⁰³ United Nations Digital Library, Opinions adopted by the Working Group on Arbitrary Detention at its 93rd session, 30 March-8 April 2022 : Opinion No. 31/2022 concerning Soulaïmane Raïssouni (Morocco), <https://digitallibrary.un.org/record/3996279?ln=en&v=pdf>

³⁰⁴ Interview with *Safir*

³⁰⁵ Report of the United Nations Special Rapporteur on the rights of freedom of peaceful assembly and of association, "Protecting the rights to freedom of peaceful assembly and of association from stigmatization", UN Doc. A/79/263, 31 July 2024.

³⁰⁶ Universal Periodic Review – Morocco, 41st Session, 4th Cycle, https://www.ohchr.org/sites/default/files/documents/hrbodies/upr/sessions/session41/ma/UPR41_Morocco_Thematic_List_of_Recommendations.doc

Clearly, Morocco is failing to adhere to these recommendations, and much stronger state action is required. As the UN Special Rapporteur on freedom of peaceful assembly and of association has noted:

“Detecting, monitoring and promptly countering stigmatizing narratives is integral to States’ obligations to respect, protect and enable the exercise of these rights. It is also paramount for preventing undue legal restrictions and repression of these freedoms, which create a cycle of repression and stigmatization... Countering stigmatization against civil society... requires a holistic approach to change the narrative through legal reforms, institutional measures, accountability, tackling discrimination and promoting different narratives.”³⁰⁷

CASE STUDY: AFAF BERNANI

“[T]he discourse against me is a political instrument” – Afaf Bernani

Afaf Bernani is a Moroccan journalist and human rights defender. In 2019, she was “aggressively pressured” by the authorities to give false testimony in the case of Moroccan journalist Taoufik Bouachrine, who was accused of sexually assaulting a colleague.³⁰⁸ After she insisted that she had witnessed no such incident, Afaf Bernani alleged that police falsified her testimony to say that Taoufik Bouachrine had also assaulted her. Excerpts of her alleged testimony were leaked to pro-Makhzen media outlets just days after her police interrogation.³⁰⁹ Speaking to Amnesty International in February 2026, Afaf Bernani said: “What unfolded was not due process. It was a systematic campaign of character assassination”.³¹⁰

Afaf Bernani refused to comply in falsifying her testimony. She filed a forgery complaint with the Court of Cassation in Rabat, which was rejected on the same day.³¹¹ Her lawyer, Mohamed Ziane, stated that no investigation took place prior to the court’s ruling.³¹² In June 2018, she was sentenced to six months in prison for perjury and defamation. Afaf Bernani fled to Tunisia in June 2019, before moving to the USA to study in February 2022. In July 2024, she was one of the 2,476 people to be officially pardoned by King Mohamed VI.³¹³

In an interview with Amnesty International, *Safir* spoke of the surprise and annoyance within the DGST when it became clear that Afaf Bernani was settling in the USA. Due to the familial and societal norms ascribed to young women in Morocco, the authorities had expected her to return.

However, Afaf Bernani told Amnesty International that her relocation to the USA did not end the harassment, it merely transformed it.³¹⁴ She described how, after taking on a volunteer position in Amnesty International USA’s student group, the online attacks against her intensified. A Moroccan individual residing in the USA published on his YouTube channel fabricated sexual allegations and claimed to have seen a pornographic video involving Afaf Bernani. “Within hours, dozens of Moroccan outlets replicated the claim – including platforms unrelated to politics,” she recalled.

For Afaf Bernani, the objective of this sustained defamation is clear:

“It is a model of governance through reputational violence. Actors abroad operate with apparent impunity while domestic media ecosystems recycle and legitimize defamatory content. It shrinks the individual to erase her credibility”.

She also identified the tactic of using women to defame other women as a strategy to “neutralize accusations of misogyny” and “fracture gender solidarity” – a practice which Kholoud Mokhtari has also denounced publicly.³¹⁵

³⁰⁷ Report of the UN Special Rapporteur on Freedom of Peaceful Assembly and of Association, Protecting the rights to freedom of peaceful assembly and of association from stigmatization, UN Doc. A/79/263, 31 July 2024, paras 114-115.

³⁰⁸ Human Rights Watch, “They’ll Get You No Matter What”: Morocco’s Playbook to Crush Dissent (previously cited).

³⁰⁹ Human Rights Watch, “They’ll Get You No Matter What”: Morocco’s Playbook to Crush Dissent (previously cited).

³¹⁰ Interview with Afaf Bernani, February 2026.

³¹¹ Guardian, “Jamal Khashoggi warned Moroccan journalist before his arrest, says wife”, 27 June 2019, <https://www.theguardian.com/world/2019/jun/27/jamal-khashoggi-warned-moroccan-journalist-before-his-arrest-says-wife>

³¹² Human Rights Watch, “They’ll Get You No Matter What”: Morocco’s Playbook to Crush Dissent (previously cited).

³¹³ Reporters Without Borders, “Morocco: Journalists Taoufik Bouachrine, Omar Radi and Soulaïmane Raïssouni Free at last”, 30 July 2024, <https://rsf.org/en/morocco-journalists-taoufik-bouachrine-omar-radi-and-soulaimane-raissouni-free-last>

³¹⁴ Interview by phone with Afaf Bernani, February 2026, “Rather than ending the harassment, geographical distance transformed it. The repression became transnational”

³¹⁵ In a Facebook post in May 2026, Kholoud Mokhtari denounced ‘smear campaigns’, including those fuelled by women against women: “Stop the defamation practiced by women against women, which was established by the patriarchy of institutions against the wives of



Screenshot of a Facebook message posted by a Moroccan female journalist, including a photo of Afaf Bernani. The post mocks Afaf Bernani and includes references to an alleged intimate video of her and Taoufik Bouachrine.

journalists and the mothers of political detainees to settle scores with them.”
<https://www.facebook.com/share/p/1Bi6yrqa3t?mibextid=wwXlfr>

The weaponization of gender is an important component of digital transnational repression targeting women human rights defenders. Research from the Citizen Lab in 2024 documented the reliance on “invasive surveillance, online harassment, sexualized threats, abuse and defamation” by authoritarian governments against women in exile and in the diaspora, including by the Moroccan government.³¹⁶

The psychological impact of these transnational smear campaigns has been significant for Afaf Bernani. At times, it has affected her ability to go about her daily life. However, her acute understanding of the psychology of what she refers to as a “tool of governance” has given her strength when she has most needed it. She knows all too well that “the discourse against me is a political instrument. It is not a definition of my identity.”

³¹⁶ See case study of Dounia Moustaslim (also known as Dounia Filali), a journalist in exile, who exposed the Moroccan security apparatus’ use of spyware against political figures and journalists: Citizen Lab, *No escape: The weaponization of gender for the purposes of digital transnational repression*, 2 December 2024, <https://citizenlab.ca/wp-content/uploads/2024/12/Report180-noescape112924.pdf>, p. 42.

9. HUMAN IMPACTS AND CHILLING EFFECT

“Hit the big ones, and the little ones will be afraid.”

Moroccan saying

The term “chilling effect” has been defined as “the negative effect any state action has on natural and/or legal persons, and which results in pre-emptively dissuading them from exercising their rights or fulfilling their professional obligations, for fear of being subject to formal state proceedings which could lead to sanctions or informal consequences such as threats, attacks or smear campaigns”.³¹⁷ The chilling effect caused by authoritarian practices, including unlawful targeted surveillance, has been well documented.³¹⁸ In Morocco, this chilling effect – whereby people feel they must self-censor – is a strategic part of the authorities’ “playbook to crush dissent”.³¹⁹ This strategy is deliberate and effective.

Both *Safir* and the human rights defenders interviewed by Amnesty International had a clear understanding that, in targeting one person, wider civil society is also targeted. Referring to Hirak El-Rif protest leader Nasser Zefzafi (see case study in Section 7.5), who remains in prison despite widespread calls for his release and credible allegations of ‘confessions’ obtained under torture, *Safir* said “no one in the region wants to end up like him”.

Human rights activist Fouad Abdelmoumni summarized this broader chilling effect: “They’re sending a message to the people, a warning. They’re saying ‘look at him! He hardly did anything and look what happened to him!’”³²⁰

“You always have to be alert and careful, to try to lessen the impact of this permanent surveillance. It’s a way of life for journalists in Morocco,” added journalist Soulaïman Raïssouni.³²¹

Achieving such self-censorship by human rights defenders is a deliberate state practice. As *Safir* put it: “There is freedom of expression in Morocco, but with limits. This freedom of expression depends on the person. It’s controlled.”³²²

Speaking with Amnesty International, journalist Hicham Mansouri spoke of the immense psychological impact of the self-censorship that surveillance imposes: “It’s very violent. A friend told me that, after years of this, the day he went into prison, it was a kind of relief.”³²³ Similarly, Fouad Abdelmoumni told Amnesty International that Morocco’s tactics of repression can lead to “either enormous self-censorship or

³¹⁷ Laurent Pech, *The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, The Rule of Law, and Fundamental Rights in the EU*, March 2021, <https://www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect>

³¹⁸ See, for example, Amnesty International, *Thailand: “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand* (Index: ASA 39/7955/2024), 16 May 2024, <https://www.amnesty.org/en/documents/asa39/7955/2024/en/>

³¹⁹ Human Rights Watch, *“They’ll Get You No Matter What”: Morocco’s Playbook to Crush Dissent* (previously cited).

³²⁰ Interview by phone with Fouad Abdelmoumni, December 2025.

³²¹ Interview by phone with Soulaïman Raïssouni, December 2025.

³²² Interview with *Safir*.

³²³ Interview in person with Hicham Mansouri, November 2025, London.

withdrawing from speaking out altogether – because we’ve seen many people who disappear from the public space from one day to the next, or who change their position”.

“Human rights defenders in Morocco are in a state of total resilience, which makes them suspicious of everything. To know you’re being filmed, followed – this is my life, my kids’ lives.” said Kholoud Mokhtari.

This state of “total resilience” comes at a huge psychological cost. Kholoud Mokhtari explained:

“When I saw that my husband was close to death [in prison], I didn’t cry, I was like a statue. I’ve lost the ability to react normally, emotionally – not just as a woman but as a human being. And that’s because I don’t live in an environment of a normal human being. It’s a way to survive.”³²⁴

The severe mental health harms inflicted due to surveillance have been recognized by courts around the world.³²⁵ In January 2026, a UK court ruled that Pegasus spyware victim Ghanem al-Masarir was entitled to more than £3 million (approximately \$4.04 million) in compensation from Saudi Arabia for psychiatric harm sustained after learning his iPhones had been hacked.³²⁶ The court heard that, even years after he was targeted, Ghanem al-Masarir continued to suffer from severe depression, was unable to work, and rarely left his home.

“The idea that we have no privacy, that power interferes everywhere and listens to everything and everyone, all the time, is an idea that is deeply ingrained in every Moroccan’s mind,” Fouad Abdelmoumni told Amnesty International.

The human rights defenders interviewed for this report all described making changes to their communication habits as a result of surveillance. Sahrawi activist El Mahjoub Maliha explained to Amnesty International how a Pegasus attack against him in 2021 still affects him today, even though he lives in Belgium:

“I haven’t visited my parents in Morocco since I found out Pegasus was on my phone. I can’t predict what Morocco will do if they were ready to spend that much money on me. There are people who refuse to call me anymore because of the Pegasus attack. Slowly, slowly, my circle has narrowed... It’s had an impact at work too. It’s completely changed the way I do my human rights work.”³²⁷

Soulieman Raissouni and his wife Kholoud Mokhtari now use Signal and Proton Mail as their primary communication channels, in an effort to keep their messages as secure as possible. But for them, even this is not a sufficient precaution, as Soulieman Raissouni explained:

“My wife and I, we have to use code for lots of our discussions, when we speak about certain things.”

Safir, knowing the tactics used by his former colleagues, described feelings of paranoia to the extent where he would check for a camera behind a mirror in a hotel room, or ask for a closed plastic bottle in a coffee shop to avoid leaving his fingerprints on a returnable glass. “I have been trying to forget my work and not bring it home with me so as to live my life normally [...] When I’m alone, I often remember details” he explained³²⁸.

A key element of the chilling effect takes the form of social and professional isolation. The human rights defenders who spoke to Amnesty International described how this tactic of repression affects their friendships and employment opportunities. Maâti Monjib explained the impact on his work as an academic:

“The majority of my colleagues talk to me in person, but sometimes they block me on WhatsApp or Facebook. It definitely makes you insecure. Members of the university community stopped working with me and stopped talking with me.”

³²⁴ Interview by phone with Kholoud Mokhtari, December 2025.

³²⁵ See, for example, Amnesty International, *Thailand: “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand* (Index: ASA 39/7955/2024), 16 May 2024, <https://www.amnesty.org/en/documents/asa39/7955/2024/en/> and Daragh Murray and others, “The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe”, 31 July 2023, *Journal of Human Rights Practice*, Volume 16, Issue 1, <https://academic.oup.com/jhrp/article/16/1/397/7234270https://academic.oup.com/jhrp/article/16/1/397/7234270https://academic.oup.com/jhrp/article/16/1/397/7234270>

³²⁶ Guardian, “Saudi Arabia ordered to pay £3m to London dissident over Pegasus spying”, 26 January 2026, <https://www.theguardian.com/world/2026/jan/26/saudi-arabia-ordered-pay-london-dissident-pegasus-spying-ghanem-al-masarir> and Royal Courts of Justice, *Ghanem Al-Masarir v Kingdom of Saudi Arabia*, Case QB-2019-003909, approved judgment, 26 January 2026, <https://caselaw.nationalarchives.gov.uk/ewhc/kb/2026/119?court=ewhc%2Fkb>

³²⁷ Interview by phone with El Mahjoub Maliha, December 2025.

³²⁸ Interview with Safir.

This can result in people not being able to work in their field at all, as has been the case for Kholoud Mokhtari: “It stopped me working. I’ve lost work and I’ve lost friends. My friends can’t get close to me. Some of them have said ‘we want to help you but we don’t know how to be near you’.”

The authorities’ public targeting of certain individuals creates an intense climate of fear which extends to wider society. As Soulieman Raissouni explained: “Many of my friends have distanced themselves from me, from us. Many members of our family too, because they think our relationship will harm them, through the authorities. And they’re right”.

DRAFT

10. SURVEILLANCE - LEGAL FRAMEWORK

“We start with the verdict”

*Safir*³²⁹

10.1 INTERNATIONAL HUMAN RIGHTS LAW AND STANDARDS ON SURVEILLANCE

The Moroccan authorities’ surveillance practices – and many of the tools it uses and are documented in this research – are in violation of international human rights law and standards. Morocco is a state party to the International Covenant on Civil and Political Rights (ICCPR), as well as most other international human rights treaties. The ICCPR protects the rights to privacy, freedom of expression, freedom of peaceful assembly, and numerous other rights affected by the state practices detailed in this report.

Privacy is both a right in itself, and a cross-cutting right, meaning that violations of the right to privacy may “affect the enjoyment of [other] human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.”³³⁰

Under international law, interference with the right to privacy is permitted only where it is “authorised by domestic law that is accessible and precise”, is in pursuit of a legitimate aim, and strictly meets the test of proportionality and necessity.³³¹ It can never be a legitimate aim to target people, their families, or social networks, for the lawful exercise of human rights, such as the exercise of the right of free expression to criticize the authorities, nor is it permissible to target people in a discriminatory manner. A measure cannot be necessary or proportionate if it is not in pursuit of a legitimate aim.³³²

Many of the tools employed by the Moroccan authorities are themselves inherently incompatible with human rights law. For example, this report documents the use of several mass surveillance tools to monitor mobile

³²⁹ Interview with *Safir*.

³³⁰ United Nations General Assembly Resolution 78/213, Promotion and protection of human rights in the context of digital technologies (2023), adopted on 22 December 2023, UN Doc. A/RES/78/213.

³³¹ UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, 28 May 2019, UN Doc. A/HRC/41/35, para. 24.

³³² See e.g. United Nations Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), 1988, at para. 3 “The term ‘unlawful’ means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.” https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FGEC%2F6624&Lang=en; United Nations Human Rights Committee, General Comment No. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant,” CCPR/C/21/Rev.1/Add. 13, (2004), at para. 6 “Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.” https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2F21%2FRev.1%2FAdd.13&Lang=en

and internet traffic at a country-wide level. Indiscriminate mass surveillance, whether of content or metadata, can never be compatible with human rights law, as it is an inherently disproportionate interference with a range of human rights.³³³

In addition, many forms of modern highly invasive spyware used by the Moroccan authorities, such as Pegasus and RCS, are incompatible with human rights as a result of their design.³³⁴ Amnesty International calls for a global ban on these forms of highly invasive spyware, because they allow unlimited access to a device and their use cannot be independently audited.

Because of these features, even a human rights compliant regulatory framework would be inadequate to prevent human rights violations linked to highly invasive spyware with these characteristics as has long been argued by Amnesty International.³³⁵ Similarly, the European Data Protection Supervisor noted that “the level of interference with the right to privacy is so severe that the individual is in fact deprived of it. In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate - irrespective of whether the measure can be deemed necessary.”³³⁶ This aligns with the reasoning presented by the former Special Rapporteur on counter-terrorism, who argued that spyware that it is incapable of being meaningfully limited in its functionality, and whose use cannot be audited independently, should be subject to a ban.³³⁷

In human rights terms, the inability of highly invasive spyware, such as Pegasus, to be limited in the amount of data it accesses means that its use cannot comport with the human rights law requirement of necessity and proportionality, since by definition it cannot be the least intrusive tool. The inability to independently audit the use of such spyware – which intentionally obscures the traces of its use – means that the human rights safeguards of independent oversight – which is also crucial to the right to remedy – cannot be effective at detecting abuses. As such, highly invasive spyware can never be used in a human rights compliant manner and should be permanently banned.

Other tools employed by the Moroccan authorities for surveillance, while they may be permissibly used in some circumstances, will also violate human rights when used in violation of the international human rights law requirements of legality, necessity and proportionality or legitimate aim. This applies not only to more advanced technologies used by Morocco, such as IMSI catchers or digital forensic tools, but also to traditional analogue methods of surveillance, such as following, or secretly recording people.

Where surveillance is deployed in violation of domestic law, such as by the informal and routine sharing of customer data between telecoms providers and security agencies, or based on laws that are unduly vague or permissive, these surveillance practices are unlawful, (see Section 10.2, below) as they fail the test of legality. Even presuming a legal basis exists, surveillance practices will be unlawful if they violate the principles of necessity or proportionality, such as by capturing more surveillance data than is needed to meet a legitimate aim, or by deploying surveillance technologies more broadly than necessary, such as by infecting all computers in an internet café with malware, or the widespread recording of the phone calls of users of a telecommunications provider.

Finally, and importantly in light of the practices described in this report, surveillance, no matter its scope or legal basis in national law, can never be lawful where it pursues an illegitimate aim, such as targeting human rights defenders, or their families, colleagues or friends, in relation to the exercise of their protected rights, including their work as human rights defenders.³³⁸

³³³ Amnesty International, *United Kingdom: Written observations submitted to the Grand Chamber of the European Court of Human Rights in Amnesty International and others' challenge to UK government mass surveillance* (Index: EUR 45/0646/2019), 3 July 2019, <https://www.amnesty.org/en/documents/eur45/0646/2019/en/>

³³⁴ UN Special Rapporteur on the on the rights to freedom of peaceful assembly and of association, *Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights*, 21 April 2026, UN Doc. A/HRC/62/45, para. 112(h)(i)(i).

³³⁵ See, for example, Amnesty International. “A Digital Prison”: *Surveillance and the Suppression of Civil Society in Serbia* (EUR 70/8813/2024), 16 December 2024, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>; Amnesty International, *Thailand: “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand* (Index: ASA 39/7955/2024), 16 May 2024, <https://www.amnesty.org/en/documents/asa39/7955/2024/en/>, Section 5.1.

³³⁶ European Data Protection Supervisor, Preliminary remarks on modern spyware, 15 February 2022, p.8

³³⁷ UN Special Rapporteur on Counter-Terrorism, Position Paper, Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, December 2022, para. 46, <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spywaretechnology-trade.pdf>

³³⁸ See e.g. United Nations Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), 1988, at para. 3 “The term ‘unlawful’ means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.” https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FGECC%2F6624&Lang=en; United Nations Human Rights Committee, General Comment No. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant,” CCPR/C/21/Rev.1/Add. 13, (2004), at para. 6 “Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure

In order to meet their obligation to respect the right to privacy, it is also crucial that the authorities have in place legal and other safeguards capable of preventing abuses of surveillance technology in practice.³³⁹ These include, but are not limited to: rigorous judicial authorization and oversight of surveillance, transparency and independent oversight of surveillance agencies and practices, notification of targets, and strict safeguards regarding the keeping, sharing and destruction of surveillance data. Safeguards must be comprehensive. By definition, safeguards which are not capable of preventing all abuses will continue to allow some, and abuses of surveillance technologies in particular, proliferate where loopholes exist that allow them.

The lack of comprehensive and adequate safeguards against abuse results not only in violations of the right to privacy of those targeted for surveillance, but also creates a chilling effect on society at large. Such chilling effects reflect a failure of states to uphold their human rights obligations.³⁴⁰ They flow predictably and directly from the failure to establish safeguards to prevent abuse.³⁴¹ It is well-established that where safeguards are lacking, for example, where people are unable to know when, how or on which basis they may be subject to surveillance, where abuses go uninvestigated, or where remedy is unattainable in practice, “widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified [...]. In such circumstances the threat of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right [to private and family life].”³⁴²

Morocco’s obligations to ensure the lawfulness of surveillance extend beyond its borders. The UN General Assembly, in its resolution 73/179, noted its deep concern “at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights”.³⁴³ Indeed, the role of unlawful surveillance in transnational repression has become the subject of increasing concern, and condemnation by UN bodies and legal experts. The Human Rights Council has adopted a resolution “Expressing its grave concern about repressive activities conducted abroad by States outside their own jurisdiction to harm, silence and intimidate human rights defenders through digital, physical and other means, including through the misuse of spyware and other intrusive surveillance software.”³⁴⁴ In a similar vein, the UN Special Rapporteur on Freedom of Expression, Irene Khan, has noted with alarm that “the targeted digital surveillance of exiled journalists has surged over the past decade, as intrusive communications software (spyware) has become available,” with particularly damaging human rights impacts on women journalists in exile.³⁴⁵ The UN High Commissioner for Human Rights recently called on states to “prevent transnational repression,” including by establishing “independent and accessible review, remedy and protection mechanisms for individuals affected by cross-border investigations or transnational surveillance, online attacks or interference with communications.”³⁴⁶

Crucially, domestic safeguards must address the interaction between surveillance systems and how these interactions can amplify human rights harms. As several UN Special Rapporteurs have noted recently: “Digital surveillance tools and methods cannot be viewed in isolation, but as elements of a complex and interconnected surveillance ecosystem.”³⁴⁷ The interconnected nature of the tools and methods employed

continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.”

https://tbineternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2F21%2FRev.1%2FAdd.13&Lang=en.

³³⁹ See, *inter alia*, “The right to privacy in the digital age,” Resolution adopted by the United Nations General Assembly on 17 December 2018 (A/RES/73/179); “Surveillance and human rights” Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/41/35 (2019).

³⁴⁰ Amnesty International, “Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects: Submission to the Special Rapporteur on Freedom of Peaceful Assembly and of Association” (Index: IOR 40/0484/2025), 18 November 2025, <https://www.amnesty.org/en/documents/ior40/0484/2025/en/>

³⁴¹ Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, Amy Stevens, “The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe,” *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, Pages 397-412, <https://doi.org/10.1093/jhuman/huad020>

³⁴² European Court of Human Rights, *Zakharov v. Russia* Application no. 47143/06, para. 171.

³⁴³ “The right to privacy in the digital age,” Resolution adopted by the United Nations General Assembly on 17 December 2018 (A/RES/73/179)

³⁴⁴ “Human rights defenders and new and emerging technologies: protecting human rights defenders, including women human rights defenders, in the digital age,” Resolution adopted by the Human Rights Council on 4 April 2025, A/HRC/RES/58/23

³⁴⁵ “Journalists in Exile,” Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/56/53 (2024)

³⁴⁶ “Protecting human rights defenders in the digital age,” Report of the United Nations High Commissioner for Human Rights, A/HRC/63/52 (2026), at para. 73(c).

³⁴⁷ “UN experts: Safeguard human freedoms from systematic digital interference, surveillance and chilling effects on civic space,” Joint Statement of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the Special Rapporteur on the situation of human rights defenders and the Special Rapporteur on the right to privacy, 27 April 2026,

by the Moroccan authorities against HRDs amplifies the harms that each tool or method might pose used in isolation, and leads to profound chilling effects on society at large.³⁴⁸ Surveillance safeguards must be able to address this in order to prevent human rights harms, including chilling effects.

10.2 MOROCCAN DOMESTIC SURVEILLANCE SAFEGUARDS AND PRACTICES IN LIGHT OF INTERNATIONAL HUMAN RIGHTS LAW AND STANDARDS

“The DGST does not care about the justice system. It totally ignores it. Like it didn't exist.”³⁴⁹

In theory, Moroccan law provides some safeguards against unlawful surveillance.

Domestically, the right to privacy is guaranteed under Article 24 of the Moroccan Constitution.³⁵⁰ Notably, - under Articles 108 and 109 of the Moroccan Code of Criminal Procedure, authorities wishing to intercept communications data in the context of criminal investigations must – in most cases not deemed urgent – obtain a prior written order from a judge which stipulates the data to be targeted, the crime suspected, and the duration of the operation (which is not to exceed four months, renewable for a total of not more than 12 months).³⁵¹

As well as being a state party to most international human rights treaties, Morocco is party to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108+”), which sets standards for the protection of data including for aims such as law enforcement and national security.

Morocco's data protection law is governed by Law 09-08, and its implementation decree 2-09-165 of May 21, 2009, which are overseen by the National Commission for the Supervision of the Protection of Personal Data (*Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel*, CNDP). However, this law has numerous gaps, including that it does not apply to personal data “collected and processed in the interest of national defence and of the internal or external security of the State, “and the Commission has failed thus far to provide remedy to victims in practice.³⁵²

Telecommunications providers in Morocco are supervised by the National Telecommunications Regulatory Authority (*Agence Nationale de Réglementation des Télécommunications*, ANRT),³⁵³ and Law No. 24-96 Relating to Postal Services and Telecommunications, which specifies operating conditions for licensed operators that include the confidentiality of communications, and the international obligations of Morocco, but also “the requirements of national defence and public safety and the prerogatives of the judicial

<https://www.ohchr.org/sites/default/files/statements/20260427-safeguard-hr-freed-syst-digi-inter-surv-chill-civic-space-sr-freedom-peaceful-en.pdf>

³⁴⁸ “Pushed into the Shadows: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association.” Study by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Gina Romero, Pete Fussey and Daragh Murray, <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

³⁴⁹ Interview with *Safir*.

³⁵⁰ Constitution of Morocco, 30 July 2011, <https://www.maroc.ma/en/morocco/constitution> (in French)

³⁵¹ Moroccan Code of Criminal Procedure (Law No. 22.01), as amended by Law No. 03.23,

<https://adala.justice.gov.ma/api/uploads/2025/12/03/%D8%B8%D9%87%D9%8A%D8%B1%20%D8%B4%D8%B1%D9%8A%D9%81%20%D8%B1%D9%82%D9%85%201.02.255%20%D8%A8%D8%AA%D9%86%D9%81%D9%8A%D8%B0%20%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%B1%D9%82%D9%85%2022.01%20%D8%A7%D9%84%D9%85%D8%AA%D8%B9%D9%84%D9%82%20%D8%A8%D8%A7%D9%84%D9%85%D8%B3%D8%B7%D8%B1%D8%A9%20%D8%A7%D9%84%D8%AC%D9%86%D8%A7%D8%A6%D9%8A%D8%A9-1764773243438.pdf#toolbar=0&statusbar=0> (in Arabic).

³⁵² General Directorate of Information Systems Security, Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement du données à caractère personnel [Law No. 09-08 relating to the protection of natural persons with regard to the processing of personal data], Article 2.4, <https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-07/loi%2009-08.pdf> (in French).

³⁵³ National Telecommunications Regulatory Agency, <https://www.anrt.ma/> (in French), (accessed on 28 July 2026).

authority”.³⁵⁴ However, as civil society observers have long pointed out, “there remains vast grey areas regarding the discretionary powers offered judges and intelligence agencies”.³⁵⁵

As the present report demonstrates, domestic safeguards are inadequate to prevent the abuse of surveillance technologies in practice and to prevent violations of both international human rights law and domestic law, especially with respect to powerful state security agencies such as DGST.

In practice, for many types of surveillance operation, no judicial written permission is obtained. This is evident in the numerous techniques *Safir* detailed, which are documented in this report, to evade scrutiny while obtaining data in official settings, such as creating a false baggage alert at an airport, giving agents time during which to use Cellebrite tools to access a device. They also include the extraction of a target’s phone when they are arrested, during the time window following the arrest but before it is officially recorded, so that there is no record of irregularity.

In addition to being carried out in violation of, or, indeed, without regard to, domestic law, DGST surveillance utilizes tools such as highly invasive spyware and mass surveillance systems that are themselves in violation of human rights law, scooping up indiscriminate amounts of data, not only from targets, but from their families and networks, and indeed society at large.

DGST surveillance fails the requirements of necessity and proportionality, routinely taking data beyond what is necessary to any legitimate purpose, infecting the PCs of entire internet cafes, and spying on the phone calls of a mobile network’s users. Crucially, DGST surveillance is unlawful because it serves no legitimate aim, but rather seeks to target HRDs for their work in defence of human rights, and their families and networks for the mere fact of being associated with them.

The DGST operate without regard for domestic legal regulations. Further legal protections, coupled with meaningful enforcement, are needed to cease the impunity with which DGST carries out unlawful surveillance against HRDs.

This unregulated and comprehensive surveillance ecosystem creates a profound chilling effect on society at large, silencing those who speak out, and sending a strong message not to do so to anyone who might consider dissenting.

“It’s very easy in Morocco, because you don’t need authorizations,” said *Safir*. “If you are a person of interest, we don’t need the law. There are no limits for us to get the work done.”³⁵⁶

10.3 THE HUMAN RIGHTS RESPONSIBILITIES OF CORPORATE ACTORS

While states have the primary duty to uphold human rights law, including through regulating companies to ensure human rights compliance, companies themselves have a responsibility to respect human rights wherever they operate in the world and across all their business activities. This is a widely recognized standard of expected conduct as set out in international business and human rights standards including the UN Guiding Principles on Business and Human Rights (UN Guiding Principles) and the OECD Guidelines for Multinational Enterprises (OECD Guidelines).³⁵⁷

This responsibility to protect human rights requires that business enterprises “avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur” as well as “seek to prevent or mitigate human rights impacts that are directly linked to their operations,

³⁵⁴ National Telecommunications Regulatory Agency, Loi n° 24-96 relative à la poste et aux télécommunications [Law No. 24-96 relating to the postal service and telecommunications], Article 10, <https://www.anrt.ma/sites/default/files/2024-09/Loi%2024-96%20consolid%C3%A9e%20site%20web%20anrt%29%20-2019%20%20-%20V7%20compil%C3%A9e.pdf?csrt=5700086543198968936> (in French).

³⁵⁵ Privacy International, State of Privacy Morocco, 26 January 2019, <https://privacyinternational.org/state-privacy/1007/state-privacy-morocco>

³⁵⁶ Interview with *Safir*.

³⁵⁷ UNOHCHR, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, 2011, endorsed by the UN Human Rights Council (UNHRC), UNHRC Resolution 17/4: Human rights and Transnational Corporations and other Business Enterprises, adopted on 16 June 2011, UN Doc. A/HRC/RES/17/4; and OECD Guidelines for Multinational Enterprises, 2011, <https://mneguidelines.oecd.org/mneguidelines>. In accordance with the UN Guiding Principles, corporate responsibility to respect human rights is independent of a State’s human rights obligations and exists over and above compliance with national laws and regulations protecting human rights. See UN Guiding Principles, Principle 11 and Commentary.

products or services by their business relationships, even if they have not contributed to those impacts.”³⁵⁸ This responsibility is independent of a state’s own human rights obligations and exists over and above compliance with national laws and regulations protecting human rights.³⁵⁹

The UN Guiding Principles clearly state that companies should use their leverage to address human rights issues with which they may be involved through linkage to another entity, even if they are not causing or contributing to any harm directly. Additionally, a company can be found to contribute to human rights impacts through, or in parallel to, third parties including other business enterprises or states due to a weak human rights due diligence process that failed to identify the risk and allow the company to address it accordingly.

In line with these international standards, companies should be conducting ongoing human rights due diligence across their entire value chain, which includes its sales to any state or non-state entity linked to its products. Tracking the conduct and behaviours of actors throughout its downstream value chain is crucial for a comprehensive human rights due diligence process, especially in the technology industry where the greatest human rights risks often lie in the usage of a particular product.³⁶⁰

States have an obligation to ensure that companies meet their responsibilities, including through regulation enforcing due diligence (including transparency) obligations, prohibiting exports that threaten human rights and by ensuring pathways to remedy for victims of human rights abuses which corporate actors cause or to which they contribute.³⁶¹

10.4 CORPORATE ACTORS’ ROLE IN UNLAWFUL SURVEILLANCE IN MOROCCO

As this report notes, Morocco has a long and well documented history of surveillance abuses, as well as inadequate safeguards in place to prevent further abuses.

These are abuses that any company providing – or brokering the provision of – technology that can be used for surveillance purposes, or otherwise lead to violations of privacy and other human rights, to Morocco should have been well aware, had they conducted adequate due diligence. They would further have been amply aware that the types of technologies in question – often including the specific products provided – are prone to abuse.³⁶² It is, moreover, clear that the risk of abuse linked to these technologies cannot be prevented or mitigated unless fundamental reforms are undertaken in Morocco, including strengthening legal protections, implementing safeguards capable of preventing abuses in practice, including by intelligence agencies, and ensuring that victims have access to remedy in practice, in order to end the culture of impunity around abuse of surveillance.

As such, any companies providing – or brokering the provision of – such technologies are contributing to unlawful surveillance described above, and the associated human rights abuses (such as defamatory smear campaigns and judicial harassment and repression) by the Moroccan authorities and must immediately cease doing so, and/or cease offering any ongoing support for such technologies. This includes all technologies that have played a role in these abuses, including IMSI catchers, digital forensic tools, and others, whether they are classed as “surveillance” tools by manufacturers or regulators. All companies who have already ceased the provision of such technologies should immediately and urgently carry out transparent investigations into their role in surveillance abuses by the Moroccan authorities and provide remedies to victims.

³⁵⁸ UNOHCHR, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, 2011, UN Doc. HR/PUB/11/04, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, Principle 13 and commentary.

³⁵⁹ OHCHR, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, 2011, UN Doc. HR/PUB/11/04, [ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf), Principle 11 including Commentary.

³⁶⁰ This rationale undergirded the European Union’s 2021 recast of its Dual-use Export Regulation to introduce an “obligation for EU Member States to control exports of cyber-surveillance items which have legitimate civilian uses - in law enforcement or network monitoring, for example - but which could also be misused for internal repression or serious violations of human rights and international humanitarian law,” https://policy.trade.ec.europa.eu/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en. Amnesty International and other civil society organizations have documented the abuse of surveillance and other technologies to target human rights defenders and violate human rights across the globe, <https://securitylab.amnesty.org/>

³⁶¹ See generally United Nations Guiding Principles on Business and Human Rights, Ch. 1.

³⁶² See, for example, Amnesty International, “*A Digital Prison*”: *Surveillance and the Suppression of Civil Society in Serbia* (Index: EUR 70/8814/2024), 16 December 2024, <https://www.amnesty.org/fr/wp-content/uploads/2024/12/EUR7088142024ENGLISH.pdf>

Additionally, companies must immediately and permanently cease the provision of any tools which cannot comply with international human rights law, such as mass surveillance systems, Pegasus and other forms of highly invasive spyware, the functionality of which cannot be limited or whose use cannot be independently audited.

The responsibility of companies to avoid causing, contributing or being linked to human rights abuses also applies to Moroccan companies, and “exists over and above compliance with national laws and regulations protecting human rights.”³⁶³ As such, domestic telecommunications companies should take measures that include, at a minimum, ensuring customer data and calls are retained only subject to legally valid requests that comply with international human rights and data protection standards, refraining from enabling unlawful surveillance such as by assisting with network injection attacks, encouraging the government to adopt rights-respecting legal and regulatory frameworks, preventing unlawful (including extra-legal) sharing of user data, carefully scrutinizing government requests to monitor or share user data or restrict content to ensure their compliance with domestic and international law and standards, challenging government orders that conflict with these legal norms, and providing public transparency regarding any such requests, and decisions and actions taken in relation to them.

Indeed, some states have acted to hold surveillance vendors accountable for abuses. In 2021, the United States, in reaction to revelations of abuses linked to NSO’s Pegasus spyware, added NSO to the “Entity List” of the Department of Commerce.³⁶⁴ Civil society actors similarly urged the European Union to adopt targeted sanctions against NSO.³⁶⁵

Finally, and importantly, corporate actors linked to human rights abuses (or the state actors that commit them) may be held liable through litigation, by victims or others. Indeed, across the world, dozens of lawsuits have been brought, including against surveillance vendors named in this report, such as NSO, FinFisher and Amesys.³⁶⁶ In a notable decision in 2026, the UK Supreme Court dismissed an appeal by Bahrain, which has been claiming state immunity against a long running lawsuit filed by two political activists, Saeed Shehabi and Moosa Mohammed for allegedly suffering psychological harm after their laptops were infected with FinSpy spyware while they were in the UK, in an operation they believe was authorized and directed by the Bahraini government.³⁶⁷ Also in 2026, four individuals linked to spyware maker Intellexa were found guilty of unlawful access to private communication systems and data, and of violating privacy and data protection laws, and given sentences of 126 years and eight months in prison each, though the sentence has been suspended pending an appeal.³⁶⁸

³⁶³ United Nations Guiding Principles on Business and Human Rights, Principle 11,

https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

³⁶⁴ Amnesty International, “USA: blacklisting of NSO Group recognises spyware abuses,” 3 November 2021,

<https://www.amnesty.org.uk/knowledge-hub/all-resources/usa-blacklisting-nso-group-recognises-spyware-abuses/>

³⁶⁵ Joint open letter by civil society organizations and independent experts urging EU-targeted sanctions against NSO Group, 3 December 2021, <https://www.amnesty.org/en/documents/eur01/5073/2021/en/>

³⁶⁶ Citizen Lab, Spyware Litigation Tracker: Legal Challenges and Formal Complaints Related to Mercenary Spyware, <https://citizenlab.ca/spyware-litigation-tracker-legal-challenges-and-formal-complaints-related-to-mercenary-spyware/>

³⁶⁷ Amnesty International, UK: Supreme Court ruling on Bahrain spyware case sends a clear message against transnational repression, 27 July 2026, <https://www.amnesty.org/en/latest/news/2026/07/uk-supreme-court/>

³⁶⁸ Amnesty International, Greece: Convictions in ‘Predatorgate’ scandal offer rare accountability in abuse of surveillance technology, 26 February 2026, <https://www.amnesty.org/en/latest/news/2026/02/greece-spyware-scandal/>

11. CONCLUSION AND RECOMMENDATIONS

For decades human rights organizations have documented repression against civil society in Morocco. Journalists and activists in particular operate in a highly restricted environment and face a variety of authoritarian practices, including unlawful surveillance and judicial harassment, often accompanied by smear campaigns. With these tactics, Moroccan authorities aim to silence dissent, attack media freedom, shrink civic space and entrench power.

This report documents how a wide array of digital surveillance tools is now central to the DGST's surveillance practices, and how they have allowed the Moroccan authorities to penetrate every aspect of the lives of human rights defenders. Use of such digital surveillance tools constitutes a key pillar of techno-authoritarianism, enabling governments to increase their control capacities through violating individual rights to privacy, assembly and expression. The human impact of such invasive forms of surveillance is made clear in the testimonies of the human rights defenders interviewed for this report.

The report also documents how a wide range of corporate actors have facilitated and enabled these techno-authoritarian practices by continuing to supply highly advanced digital surveillance technologies to Morocco, while ignoring evidence of how such tools have been used to violate human rights. For example, since 2017 Amnesty International has published multiple investigations documenting the unlawful targeting of Moroccan civil society with Pegasus spyware, which continued until at least November 2021. NSO Group claims that Pegasus spyware is used only to "investigate terrorism and crime". Numerous investigations by Amnesty International and other civil society organizations around the world have demonstrated that in fact Pegasus spyware has repeatedly been used by governments to target human rights defenders, journalists, and other members of civil society. This research demonstrates that, at least in the case of Morocco, civil society were not merely occasional victims but were in fact the primary target of the DGST once they acquired the spyware system, making up almost two thirds of the targets in the initial four months of its operation. This report further documents that the involvement of NSO Group does not stop at the point of purchase. Pegasus spyware is not operated autonomously by a government customer but instead relies on maintenance and support by NSO Group to enable its ongoing functioning.

The combination of unlawful surveillance, judicial harassment and smear campaigns creates a profound chilling effect on human rights defenders, and on society at large. The weaponization of technology is key to this three-part threat: With no way to know when they are being observed and recorded, facing unknown risks for family and friends, concerned with public shaming or even imprisonment if they speak out, many fear to do so, and the space for dissent grows ever more hostile.

And yet, many do continue to speak out and attempt to hold those in power to account. Their cases are highlighted in this report. Their stories underscore the urgent need for the Moroccan authorities to put an end to the impunity enjoyed by the DGST, to reform their laws and practices, and to make Morocco a safe space for journalists and human rights defenders.

The findings of this report highlight the Moroccan authorities' failure to protect and uphold human rights defenders' basic human rights, as guaranteed under international law. This report also illustrates the key role of whistleblowers in disclosing human rights abuses. Amnesty International urges the Moroccan authorities and other relevant actors to immediately adopt the following recommendations:

11.1 TO THE MOROCCAN AUTHORITIES

- Release people imprisoned solely in connection with the lawful exercise of their human rights.
- Uphold the right to privacy and the rights to freedom of expression, association and peaceful assembly, as guaranteed by Morocco's Constitution and international human rights law and standards, including the International Covenant on Civil and Political Rights.
- Immediately cease unlawful surveillance of human rights defenders and journalists lawfully exercising their human rights and respect and ensure their right to privacy.
- Ensure an independent, effective and systemic investigation into the DGST, including all reported cases of unlawful surveillance, hold all those responsible to account and provide for effective remedies for victims, including meaningful pathways for judicial redress, for physical and mental harm, as well as loss of livelihood.
- Impose a ban on highly invasive spyware, whose functionality cannot be limited to only those functions that are necessary and proportionate to a specific use and target, or whose use cannot be independently audited.
- Ensure that data from surveillance operations is not shared unlawfully with other authorities or with media or private entities engaging in smear campaigns against surveillance targets.
- Reform the Data Protection Law (No. 09-08 of 2009) to ensure that the CNDP is empowered to investigate all data protection issues, including those related to law enforcement and national security.
- Disclose publicly information about all previous, current, or future contracts with private surveillance companies, including those with NSO Group, Hacking Team, Memento Labs, Verint, Amesys, Cellebrite, Interionet, and other companies and technologies named in this report.
- Undertake legislative reforms needed to implement a human rights regulatory framework governing surveillance that ensures effective oversight of the actions of the DGST and other security agencies and accountability for any violations. This domestic human rights regulatory framework must ensure, at a minimum, that:
 - Surveillance is governed by precise and publicly accessible laws.
 - Surveillance is authorized by a competent, independent and impartial judicial body, affects only specified persons, and that such authorization includes limitations on time, manner, place and scope of surveillance.
 - Authorized digital surveillance is subject to detailed record keeping, in accordance with documented legal processes for a warrant, and targets are notified as soon as practicable without jeopardizing the purpose of surveillance.
 - Agencies authorized to conduct surveillance and judicial authorities authorizing them prepare meaningful assessments to ensure that the objectives of surveillance could not be achieved with means that are less intrusive on human rights.
- Until such a framework is implemented, a moratorium on the purchase, sale, transfer and use of surveillance equipment should be enforced
- Carry out an investigation into state support for online smear campaigns attacking human rights defenders and journalists for their work and ensure that it ceases. Ensure that there is no participation or instigation by state actors in defamatory smear campaigns against human rights defenders and journalists, including on social media, and take steps to protect human rights defenders from such campaigns in media outlets.
- Ensure that telecommunications providers are not prevented from exercising transparency regarding their roles in state surveillance activities, including such as by disclosing data regarding state requests for cooperation, interception or access to customer data.

- Take concrete action to counteract the chilling effect and create a safe and enabling environment where civil society members, activists and journalists are able to freely and safely exercise their rights to freedom of expression and assembly in digital spaces, without fear of harassment, intimidation and violence, in line with international standards and safeguards:
 - End all criminal proceedings against all people charged solely for their involvement in peaceful protests or for exercising their right to freedom of expression.
 - Establish and enforce codes of conduct on public communications for officials to ensure public officials do not engage in online harassment and smear campaigns against activists, journalists and human rights defenders.

11.2 TO ALL STATES

- Deny export authorization of spyware, digital forensics tools, and other privacy-invasive technology to Morocco until such time as there has been a thorough, independent and effective investigation into unlawful surveillance of journalists, political activists and human rights defenders, and a system of human rights safeguards is in place capable of preventing human rights abuses in practice.
- Prohibit companies from producing, selling, transferring or supporting highly invasive spyware, the functionality of which cannot be limited and whose use cannot be independently audited.
- Utilise unilateral and multi-lateral mechanisms to ensure accountability for spyware and other technology companies complicit in human rights abuses.
- Ensure strong enforcement of export control regulations for all surveillance technologies.
- Ensure that surveillance companies conduct human rights due diligence in relation to their operations, including on the use of their products and services by other companies beyond the first tier in their value chain.
- Take meaningful steps to ensure transparency and accountability regarding human rights due diligence regulation and practices, including by granting public access to beneficial ownership information of companies registered in their jurisdiction.
- Pass mandatory human rights due diligence law that requires all companies to adequately address all possible and actual adverse impacts that their operations, products and services may have along the entire value chain, including on rights holders. This law should ensure that this human rights due diligence is conducted early in the process and on an ongoing basis, given that risks and impacts may shift over time.

11.3 TO STATES FROM WHICH SURVEILLANCE OR OTHER PRIVACY-INVADING TECHNOLOGY IS EXPORTED, SOLD OR BROKERED

- Conduct an investigation into the export, sale, transfer or brokering of technology linked to human rights abuses in this report, and revoke export licences where there is evidence or significant risk of its link to human rights abuses.
- Prevent companies from brokering or otherwise facilitating the sale, transfer or support of surveillance and other privacy-invading technology to Morocco until such time as there has been a thorough, independent and effective investigation into unlawful surveillance of journalists, political activists and human rights defenders, and a system of human rights safeguards is in place capable of preventing human rights abuses in practice.

11.4 TO COMPANIES INVOLVED IN SUPPLYING SURVEILLANCE AND OTHER PRIVACY-INVADING TECHNOLOGY TO MOROCCO

- Halt all sales, exports and transfers of all surveillance technologies to Morocco, as well as all brokering or other support for such sales, transfers or support, until such time as there has been a thorough, independent and effective investigation into unlawful surveillance of journalists, political activists and human rights defenders, and a system of human rights safeguards is in place capable of preventing human rights abuses in practice.
- Ensure transparency regarding sales and contracts, as well as the volume, nature, value, destination and end-user of surveillance transfers.
- Implement adequate human rights due diligence processes, as set out in international business and human rights instruments, such as the UN Guiding Principles on Business and Human Rights to ensure your activities, or those of your subsidiaries, sub-contractors and suppliers respect the rights of human rights defenders and do not hinder their legitimate work.
- Conduct consultations with rights holders before signing contracts in countries.
- As part of the responsibility to conduct human rights due diligence, carry out robust human rights risk assessments for all proposed transfers, which should be scrutinized by export authorities and made public.
- Implement contractual protections against human rights abuses.
- Have an adequate notification process for reporting misuse of technology and grievance mechanisms.
- Implement robust mechanisms for compensation of targets of unlawful surveillance or other forms of redress.
- Immediately halt the sale, transfer and/or support of highly invasive spyware, the functionality of which cannot be limited or independently audited, as well as all brokering or other support for such sales, transfers or support.

11.5 TO TELECOMMUNICATIONS PROVIDERS (MOBILE AND INTERNET) OPERATING IN MOROCCO

- Carry out adequate human rights due diligence in order to identify, prevent, mitigate and account for adverse human rights impacts, including in relation to surveillance, in particular by thoroughly assessing the risks of unlawful data sharing, or participation in state surveillance operations such as network injection attacks, and making risk assessments public.
- Ensure that customer data and calls are retained only subject to legally valid requests that comply with international human rights and data protection law and standards, and are not subject to indiscriminate retention or extra-legal sharing with authorities.
- Resist state demands for surveillance data, and regularly publish comprehensive transparency reports detailing government requests.
- Reinforce engagement and collaboration with all stakeholders working to prevent unlawful surveillance.
- Develop accessible and safe grievance mechanisms through which complaints regarding surveillance technology and its use can be addressed effectively. These mechanisms should be available in all countries and measures must be taken to ensure the mechanism is accessible to all.

12. ANNEXES

The following annexes include technical records and material evidence which support claims made in this report. This evidence is intended to be useful for a technical audience and spyware accountability researchers.

12.1 CIRCLES / NSO GROUP VPN SERVER CERTIFICATES

The following table of internet scan shows that Moroccan VPN server was first placed online in August 2017 on a network tied to Circles Bulgaria, a company owned by NSO Group parent company Q Cyber Technologies. The VPN server then transferred from Bulgaria to Morocco, first coming online in Morocco in September 2017.

Table 3: VPN server certificate visible in Bulgaria and then later in Morocco (MDTI data)

IP ADDRESS	COUNTRY	CERTIFICATE	FIRST SEEN	LAST SEEN
84.1.246.229	Bulgaria	c31688be493b337ec8428f8a55a8b0d3b1ddfcfd	2017-08-01	2017-08-01
84.1.246.230	Bulgaria	c31688be493b337ec8428f8a55a8b0d3b1ddfcfd	2017-08-01	2017-08-01
84.1.246.231	Bulgaria	c31688be493b337ec8428f8a55a8b0d3b1ddfcfd	2017-08-01	2017-08-01
105.145.40.26	Morocco	c31688be493b337ec8428f8a55a8b0d3b1ddfcfd	2017-09-12	2021-03-09
105.145.40.27	Morocco	c31688be493b337ec8428f8a55a8b0d3b1ddfcfd	2017-09-12	2021-01-11
105.145.40.28	Morocco	c31688be493b337ec8428f8a55a8b0d3b1ddfcfd	2017-09-12	2021-01-19

The following table shows how a similar pattern of observed for a Circle VPN server first deployed in Bulgaria before being transferred to the UAE and deployed at the same time as a Pegasus system for the Emir of Dubai (codename “dutton”).

Table 4: Certificates on Bulgarian IP 84.1.246.230 tied to Q Cyber Technologies

CERTIFICATE	CERTIFICATE NAME	CERT ISSUED	FIRST SEEN	FIRST SEEN CLIENT
CCFD03A1DDB096 1B3360E6D76B366 2FBB7781037	client-dutton-dolce VPN Certificate	2016-10-27	2016-11-07	2016-12-05 91.75.44.86 (UAE)
C31688BE493B337 EC8428F8A55A8B0 D3B1DDFCFD	localhost	2017-07-31	2017-08-01	2017-09-12 105.145.40.27 (Morocco)

12.2 VERINT SALES PROPOSALS TO MOROCCO

EXP. BOOKING Q (OPPORTUNITY) (OPPORTUNITY)	OPPORTUNITY NAME (OPPORTUNITY) (OPPORTUNITY)	\$US AMOUNT (OPPORTUNITY) (OPPORTUNITY)	PROPOSAL TYPE (OPPORTUNITY) (OPPORTUNITY)	EXISTING PRODUCT	PRIMARY PB	COUNTRY (OPPORTUNITY) (OPPORTUNITY)	ACTUAL CLOSE DATE (OPPORTUNITY) (OPPORTUNITY)	STATUS REASON (OPPORTUNITY) (OPPORTUNITY)
2014/Q4	Cannelle Sauvage	14,000,000	New System	Reliant 12	CI	Magazine	25.12.14	Won
2016/Q3	Canelle 100G Upgrade	1.651.500	Other	Reliant 12	CI	Magazine	19.10.16	Won
2016/Q3	Canelle Shaver Maintenance	1.700.000	Maintenance	Reliant 12	CI	Magazine	19.10.16	Won
2016/Q3	Canelle Shaver Maintenance	1.700.000	Maintenance	VANTAGE 6.0	CI	Magazine	30.07.16	Canceled
2016/Q4	White Alpha	1.700.000	New System	GI2X	TI	Magazine		In Progress
2017/Q1	Canelle Shadow	5000000	New System	EPI Premium	CI	Magazine		In Progress
2017/Q2	Canelle Cyclone	2500000	New System	TPS	Cyber	Magazine		In Progress
2017/Q2	Canelle SUN	8000000	New System	VANTAGE X	CI	Magazine		In Progress
2017/Q2	Canelle Hurricane	5000000	New System	Verint Cyber Security Center	Cyber	Magazine		In Progress

12.3 ANNEX: PROFILES OF PEOPLE INTERVIEWED FOR THIS REPORT

Fouad Abdelmoumni is a Moroccan economist and veteran human rights defender and activist. Now living in Switzerland, he has been subjected to state surveillance (including Pegasus spyware), defamation and judicial harassment. In March 2025, a Casablanca court sentenced him to six months in prison in his absence following a Facebook post about Morocco's use of Pegasus spyware.

Afaf Bernani is a journalist, human rights defender and former [report-reporter](#) at Akhbar Al Yaoum newspaper. In 2019, she was pressured by the authorities to give false testimony in the case of Moroccan journalist Taoufik Bouachrine. In June 2018, she was sentenced to six months in prison for perjury and defamation. Afaf Bernani fled to Tunisia in June 2019, before moving to the USA in February 2022, where she still resides. In July 2024, she was one of the 2,476 people to be officially pardoned by King Mohamed VI.

Mohamed Majaoui is a teacher and activist from Al Hoceima, a city in the Rif region. He was sentenced to five years in prison for his role in the Hirak El-Rif protests in 2017. He currently leads the Al Hoceima chapter of the Moroccan Association of Human Rights (AMDH).

El Mahjoub Maliha is a Sahrawi human rights defender and is currently the head of external relations at the Sahrawi Human Rights Defenders Collective (CODESA). He lives in Belgium. Following the Pegasus Project revelations of 2021, it was revealed that El Mahjoub Maliha's phone had been infected with Pegasus spyware while he was living in Belgium.

Kholoud Mokhtari is a Moroccan screenwriter and human rights activist, living in Morocco. She is married to journalist Soulaïman Raïssouni. She has been subjected to surveillance, both inside and outside of Morocco, harassment and defamation in the press.

Maâti Monjib is a Moroccan university professor, historian, media writer, human rights defender and political activist. He is also the former president of the association Freedom Now, which defends the right to freedom of association in Morocco, and co-founder of the Moroccan Association of Investigative Journalism (AMJI). In October 2019, Amnesty International confirmed that his phone was targeted and infected with Pegasus spyware. He has also been subjected to judicial harassment and frequent smear campaigns.

Omar Radi is an investigative journalist and activist from Morocco. He is a founder and former journalist at Le Desk, an independent Moroccan publication.³⁶⁹ He has worked with several national and international media outlets, including Atlantic Radio, Le Journal Hebdomadaire, Telquel and Lakome. Omar Radi's work focuses on political investigation and the relations between political and economic powers in Morocco. As of February 2026, he is residing in Europe.

Soulaïman Raïssouni is a Moroccan journalist and human rights defender who has been a vocal critic of the authorities for many years. He was editor-in-chief of the now-closed independent newspaper Akhbar al-Youm. He has faced intensive surveillance, judicial harassment and smear campaigns. In July 2021, he was sentenced to five years in prison on charges of sexual assault. He was released by royal pardon in July 2024.

Ali Salem Tamek lives in Laayoune, Western Sahara, and is president of CODESA. He is a prominent human rights defender, independence activist and trade unionist. He has faced routine harassment and persecution in his attempt to monitor and denounce abuses by Moroccan authorities.

Hicham Mansouri is a Moroccan journalist, author and co-founder of AMJI. In 2015, he was imprisoned under trumped-up charges of "adultery" and "sexual exploitation" after a trial which did not meet international standards. Amnesty International considered him to be a prisoner of conscience.³⁷⁰ He spent 10 months in prison before claiming asylum in France. In June 2021, Amnesty International identified that his devices had been hacked over the previous months with Pegasus spyware in France after he was granted asylum. He continues to live in France, from where he co-founded and edits Hawamich, an independent Moroccan media platform.³⁷¹

³⁶⁹ Le Desk, <https://ledesk.ma/> (in French)

³⁷⁰ Amnesty International, *Morocco: journalist jailed for press freedom work* (Index: MDE 29/1489/2015), 22 April 2015, <https://www.amnesty.org/en/documents/mde29/1489/2015/en/>

³⁷¹ Hawamich, <https://hawamich.info/> (in Arabic)

DRAFT

**AMNESTY INTERNATIONAL
IS A GLOBAL MOVEMENT
FOR HUMAN RIGHTS.
WHEN INJUSTICE HAPPENS
TO ONE PERSON, IT
MATTERS TO US ALL.**

CONTACT US



contactus@amnesty.org



+44 (0)20 7413 5500

JOIN THE CONVERSATION



www.facebook.com/amnesty



@Amnesty

'WE START WITH THE VERDICT'

INSIDE MOROCCO'S SURVEILLANCE MACHINE

This report documents the surveillance ecosystem that enables the Moroccan authorities to use repressive tactics to harass, discredit and ultimately silence human rights defenders. It outlines the role of Morocco's domestic intelligence service, the Direction Générale de la Surveillance du Territoire (DGST), in conducting surveillance operations against civil society.

These operations are often accompanied by smear campaigns in state-aligned media outlets. The techno-authoritarian practices used by the DGST, and documented in this report, have been facilitated and enabled by various corporate actors.

The report also contains a comprehensive analysis of the Pegasus spyware system, and how it has been used by Morocco to target human rights defenders and journalists, both inside Morocco and internationally.