



“WE START WITH THE VERDICT”

INSIDE MOROCCO’S SURVEILLANCE MACHINE
EXECUTIVE SUMMARY

AMNESTY
INTERNATIONAL



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 2020

by Amnesty International Ltd

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

Index: MDE 29/1481/2026

Original language: English

amnesty.org



Cover image: © Rectangle / Evan Grothjan

AMNESTY
INTERNATIONAL



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 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 sullying 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 commenters 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 it 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 have been 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

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. These tactics 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, peaceful 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.

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.

Amnesty International wrote to the Moroccan authorities with a summary of our findings one month prior to publication and invited their response. The Moroccan authorities did not reply.

Prior to publication, Amnesty International wrote to the companies featured in the report with our key findings related to their operations. Verint replied to state that "Verint divested this line of business on Feb. 1, 2021. Media inquiries should be referred to Cognyte Software Ltd." Amnesty International did not receive a reply from any of the other companies.

KEY 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.



**AMNESTY INTERNATIONAL
IS A GLOBAL MOVEMENT
FOR HUMAN RIGHTS.
WHEN INJUSTICE HAPPENS
TO ONE PERSON, IT
MATTERS TO US ALL.**

CONTACT US



info@amnesty.org



+44 (0)20 7413 5500

JOIN THE CONVERSATION



www.facebook.com/AmnestyGlobal



[@Amnesty](https://twitter.com/Amnesty)

“WE START WITH THE VERDICT”

INSIDE MOROCCO’S SURVEILLANCE MACHINE

EXECUTIVE SUMMARY

This report documents the surveillance ecosystem that enables the Moroccan authorities to use repressive tactics to harass, discredit and ultimately silence human rights defenders. The report 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.