

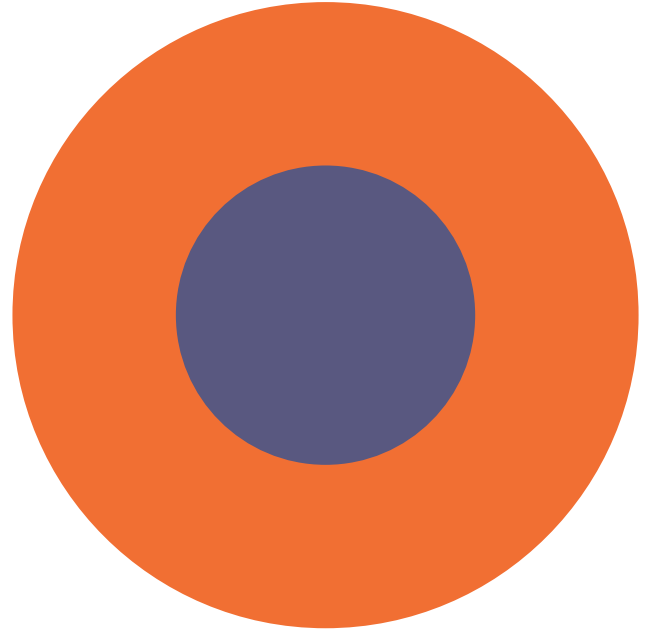


HuMENA For Human Rights and Civic Engagement  
HuMENA pour les Droits de l'Homme et l'Engagement Civique  
هيومينا لحقوق الإنسان والمشاركة المدنية

# Eyes Everywhere:

The State Surveillance of Human  
Rights Defenders in Jordan





# Eyes

# Everywhere:

## The State Surveillance of Human Rights Defenders in Jordan

HuMENA For Human Rights and Civic Engagement © 2024



HuMENA For Human Rights and Civic Engagement  
HuMENA pour les Droits de l'Homme et l'Engagement Civique  
هيومينا لحقوق الإنسان والمشاركة المدنية

[www.humena.org](http://www.humena.org)

15/4 Rue Alphonse Hottat | Brussels 1050 | Belgium

# Table of Contents

<b>1. Executive Summary</b>	<b>1</b>
<b>2. Introduction</b>	<b>2</b>
2.1. Background	2
2.2. Scope	2
2.3. Methodology	2
<b>3. Legal Context</b>	<b>3</b>
3.1. Surveillance in Jordanian Legislation	3
3.2. Privacy Regulation	4
<b>4. Surveillance in Practice</b>	<b>4</b>
4.1. Use of Pegasus Spyware in Jordan	5
4.2. Other Known Surveillance Capabilities and Actors	6
4.3. Public Responses	7
<b>5. Impact on Human Rights Defenders</b>	<b>8</b>
5.1. Legal Consequences	8
5.2. Behavioral Impact	11
<b>6. Recommendations</b>	<b>12</b>
<b>7. Conclusion</b>	<b>13</b>

# 1. Executive Summary

This report examines the rise in state surveillance and harassment of human rights defenders, including journalists and other civil society actors, in Jordan, emphasizing the significant impact of these practices on privacy, free expression, and peaceful assembly.

Due to high levels of self-censorship driven by fear of retaliation and the widespread chilling effect caused by severe surveillance, there is minimal reporting on this issue. In the context of curtailed media activity, this report aims to present a detailed account of the state of surveillance on human rights defenders in Jordan, challenging the prevailing silence.

Despite the privacy protections outlined in Jordan's constitution and the recently passed Personal Data Protection Law, the report reveals that surveillance is facilitated by various laws, including the Cybercrime Law, the Telecommunications Law, and the Anti-Terrorism Law. These laws permit extensive network, communication, and social media surveillance.

The report also documents the increasing repression of civic space in Jordan, noting the widespread use of notorious spyware such as Pegasus against human rights defenders since 2019, and the expansion of surveillance capabilities within Jordanian security agencies.

In conclusion, the report offers several recommendations for the Jordanian government, emphasizing the need for an independent investigation into spyware use, the establishment of accountability mechanisms for victims, and the repeal of the Cybercrime Law. It also calls for an end to the intimidation of human rights defenders by security authorities. Additionally, the report provides recommendations for technology vendors and social media companies and ends with digital security advice for human rights defenders.

# 2. Introduction

## 2.1. Background

Over the past decade, Jordanian state authorities have continuously and systematically proceeded to crush civic space through repressive legislation (Cybercrime Law, Press and Publications Law, Societies Law, Crime Prevention Law) and extrajudicial practices and procedures. In the last 12 months alone, Jordan has seen a steep increase in the detention of journalists and human rights defenders related to their peaceful work and assembly, and an increase in the use of digital surveillance technologies to facilitate these coercive practices.

In its 2024 (as well as 2023) Freedom in the World report, DC-based think tank Freedom House quantified the state of freedoms in Jordan as “not free,” and the state of Internet freedoms as “partly free.”<sup>1</sup> These findings correlate with Reporters Without Borders’ rating which publishes a yearly country-by-country index on press freedoms, placing Jordan 132nd out of 180 countries in terms of press freedoms (Jordan ranked lower in 2023, coming in 146th).<sup>2</sup> In 2023, Civicus classified Jordan’s civic space as “repressed.”<sup>3</sup>

## 2.2. Scope

This report examines the digital surveillance of human rights defenders in Jordan over the past 5 years and its impacts on civic space nationally. Digital surveillance encompasses surveillance of mobile devices, network tapping, as well as surveillance of personal accounts particularly social media accounts.

This report applies the UN OHCHR’s definition of human rights defenders as per their declaration on human rights defenders.<sup>4</sup>

## 2.3. Methodology

The research relies on primary and desk research on surveillance in Jordan, uncovering and documenting cases of digital surveillance of human rights defenders, and cataloging state-sponsored surveillance technologies used against civil society.

---

<sup>1</sup> [Jordan: Country Profile | Freedom House](#)

<sup>2</sup> [Jordan | RSF](#)

<sup>3</sup> [Jordan - Civicus Monitor](#)

<sup>4</sup> [Declaration on human rights defenders | OHCHR](#)

# 3. Legal Context

## 3.1. Surveillance in Jordanian Legislation

In Jordan, an array of regulations has been put forward and employed to surveil citizens. These have had a significant impact on the rights to free expression and peaceful assembly. This section delves into key regulations that are regarded to have profound implications for these freedoms, complementing later sections that illustrate their detrimental impact on human rights defenders.

In August of 2023, Jordan enacted drastic amendments to the Cybercrime Law which many local and international independent bodies have deemed as highly repressive with many experts arguing its unconstitutionality<sup>5</sup> as well as its incompatibility with international conventions ratified by Jordan.<sup>6</sup> Whilst the Jordanian government has defended the law as protecting the online space and an attempt to tackle mis and disinformation,<sup>7</sup> its broad definitions have been used to silence dissent.

Article 36 of the 2023 Cybercrime Law establishes regulations for social media platforms. It requires any online platform with over 100,000 subscribers in Jordan to set up an office in the country to handle requests from legal and administrative authorities regarding user accounts or content removal.<sup>8</sup> Non-compliant platforms may face restrictions, including bans on advertisements and gradual reductions in traffic bandwidth.<sup>9</sup>

Article 12 of the law criminalizes the use of virtual private networks (VPNs) and other tools designed to circumvent or anonymize internet activity if used with the “intent to commit a crime.” Article 12 of the law criminalizes the use of virtual private networks (VPNs) and other tools designed to circumvent or anonymize internet activity if used with the intent to commit a crime.

Moreover, the Anti-Terrorism Law of 2006, specifically Article 4, threatens privacy rights under the guise of protecting public safety and security. The Article allows for surveillance of individuals if the Prosecutor General receives «reliable information» suggesting that the person or a group is connected to any terrorist activity. However, the law does not define what constitutes «reliable information» or «terrorist activity.»<sup>10</sup>

As per the Telecommunications Law, telecommunication providers in Jordan are legally compelled to cooperate with authorities and monitor user communications. The law obliges telecommunication providers specifically to take measures required to retain and submit user communication data upon judicial or administrative order.<sup>11</sup>

---

<sup>5</sup> [مشروع قانون الجرائم الإلكترونية في الأردن... العودة إلى الوراء مرة أخرى | معهد الجزيرة للإعلام](#)

<sup>6</sup> [Jordan: Concerns over cybercrime legislation and shrinking of civic space | OHCHR](#)

<sup>7</sup> [New Jordanian cybercrime law criminalizes ‘fake news’ online - Committee to Protect Journalists](#)

<sup>8</sup> [Full Text in English of the Cybercrime Law of 2023](#)

<sup>9</sup> [Jordan: Scrap Draconian Cybercrimes Bill | Human Rights Watch](#)

<sup>10</sup> [Data protection policy void threatens privacy rights of citizens and refugees in Jordan](#)

<sup>11</sup> [Jordan: Telecommunications Law No. 131995/ | Public Private Partnership](#)

Following a directive from the Telecommunications Regulatory Commission (TRC), Jordan mandates that individuals purchasing SIM cards must submit their biometric data. Foreigners are required to present a passport for identification.

Finally, the Code of Criminal Procedures grants broad powers to the public prosecutor to search homes, conduct raids, and confiscate all forms of correspondence and communication mediums that «may assist in revealing the truth.»

## 3.2. Privacy Regulation

Article 18 of the Jordanian Constitution stipulates that “All postal, telegraphic, and telephone communications, as well as other forms of communication, are considered confidential and cannot be monitored, reviewed, intercepted, or confiscated except by judicial order in accordance with the provisions of the law.”

The Telecommunications Law further states that “telephone calls and private telecommunications shall be considered confidential and may not be violated under legal liability.”

After nine years of drafting, the Jordanian Council of Ministers passed the Personal Data Protection Law in August 2023. This law regulates how personal data is collected, used, and published within the country and by services operating there. Civil society organizations have criticized the law for failing to ensure the independence of the proposed Data Protection Authority, which includes members of the government and security forces. Additionally, the law’s vague language allows for interpretations that could undermine the privacy protections intended by its enactment.

---

12 [Timeline of SIM Card Registration Laws | Privacy International](#)

13 [قانون أصول المحاكمات الجزائية وتعديلاته رقم 9 لسنة 1961](#)

14 [Jordanian Constitution](#)

15 [Data protection policy void threatens privacy rights of citizens and refugees in Jordan](#)

16 [Jordan passes flawed data protection law - Access Now](#)

# 4. Surveillance in Practice

## 4.1. Use of Pegasus Spyware in Jordan

From 2019 until late 2023, independent forensic researchers identified 39 unique cases of Pegasus spyware infections in Jordan.<sup>17 18</sup> Pegasus is a spyware developed by the Israeli company NSO that installs itself on a device – without the target’s knowledge or consent – to spy on the target. Spyware can see virtually everything stored on the device (messages, files, photos, passwords, browsing history), conduct live surveillance (through microphone and camera), and transmit this data to the surveilling party.

In Jordan, targets have included politicians, members of parliament, and members of the Royal Court; however, the majority were political activists, human rights defenders, lawyers, and journalists.<sup>19</sup>

Of the 39 targets identified over the last four years, 16 have gone public about their cases. Among these 39 uncovered cases, 37 involve civic space actors, with journalists forming the majority of the targets. Specifically, these include:

- **18 journalists:** including two investigative journalists working for the Organized Crime and Corruption Reporting Project (OCCRP); Daoud Kuttub, founder of Radio Al-Balad and AmmanNet; Rai al-Youm journalist Suhair Jaradat; and Hosam Gharaibeh, director of Husna Radio.
- **9 human rights lawyers:** including five from the National Forum for the Defense of Freedoms, constitutional expert Omar Atout, and Malik Abu Orabi.
- **6 political activists:** including Ahmad Neimat, a member of the Jordanian Hirak.
- **4 civil society members:** including two individuals from the Jordan-based regional office of Human Rights Watch,<sup>20</sup> and Manal Kasht, founder of Shabbat, a local civil society organization seeking to empower women in politics.

Pegasus is known to be sold exclusively to governments.<sup>21</sup> Although it is difficult to attribute attacks to specific states, the Citizen Lab, a research group at the Munk School of Global Affairs at the University of Toronto, identified two main Pegasus operators in Jordan in their 2022 report. The first operator has been active since at least December 2018, and appears to primarily conduct targeted surveillance within Jordan, with some operations extending to the region (Iraq, Lebanon, and Saudi Arabia). The latter, active since December 2020, appears to operate entirely within Jordan.

While there is no tangible evidence to date directly identifying states purchasing and operating Pegasus spyware in Jordan to target activists, lawyers, and journalists, a 2021 news report from Axios revealed ongoing negotiations between NSO and Jordanian intelligence officials. Additionally,

---

17 [Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware - The Citizen Lab](#)

18 [Unsafe anywhere: women human rights defenders speak out about Pegasus attacks](#)

19 [Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan](#)

20 [Spyware Targets Human Rights Watch Staff in Jordan](#)

21 [Pegasus Spyware: A Grave Threat to Journalists in Southeast Asia | Al Jazeera Media Institute](#)

previous reports have disclosed that NSO Group uses code names for its clients, with «Jaguar» reportedly being the code name for Jordan.<sup>22</sup>

## 4.2. Other Known Surveillance Capabilities and Actors

Evidence and reports indicate that Jordan possesses various other digital surveillance capabilities and practices different forms of surveillance, from basic online patrolling to targeted interception of communications.

A year following the enactment of the Cybercrime Law in Jordan, the Cybercrime Unit of the Public Security Directorate launched its “online patrols” to keep watch of content published on social media platforms in Jordan and alert of content and accounts violating Jordanian laws.<sup>23 24</sup>

Moreover, Jordanian telecommunication companies and mobile operators are known to possess deep packet inspection (DPI) capabilities, specifically through the PacketLogic device<sup>25</sup> developed and distributed by the Canadian company Sandvine Inc.<sup>26</sup> DPI technology allows telecommunication providers to closely examine all the data passing through its networks. In Jordan, it has primarily been used for precise censorship of online services,<sup>27</sup> it can also, in theory, be employed for extensive surveillance of network traffic.

Jordan has attempted to expand its surveillance capabilities as reports and leaks have revealed the state’s interest in or procurement of spying technologies over the years.

In 2015, emails released by WikiLeaks revealed that Jordan’s General Intelligence Directorate was in correspondence with the Italian surveillance vendor Hacking Team (HT), seeking information about HT’s Remote Control System, spyware that facilitates targeted surveillance on smartphones and computers.<sup>28</sup>

In late 2023, an investigation by the European Investigative Collaborations (EIC) media network, in technical collaboration with Amnesty International’s Security Lab, found that Intellexa Alliance products had been sold to 25 countries, including Jordan.<sup>29</sup> Intellexa manufactures a suite of products designed for mass network surveillance and targeted device surveillance, including the well-known Predator spyware.

Finally, the recently published global database of surveillance tech, Surveillance Watch, observed additional surveillance technology vendors targeting individuals in Jordan. Besides those previously mentioned, the initiative identifies the US-based company Procera Networks, which provides deep packet inspection technology; the Russia-based company Protei, which offers surveillance

---

22 [Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles - The Citizen Lab](#)

23 [الأردن.. دوريات إلكترونية لملاحقة حسابات المسئنين | أخبار الجزيرة نت](#)

24 [State of Privacy Jordan](#)

25 [Blocking Clubhouse in Jordan: A Quick Analysis of Internet Censorship Methods in Use](#)

26 [Sandvine Technology Used to Censor Web in More Than a Dozen Nations - Bloomberg](#)

27 [Jordan: Measuring Facebook live-streaming interference during protests | OONI](#)

28 <https://wikileaks.org/hackingteam/emails/emailid/616353>

29 [Global: 'Predator Files' investigation reveals catastrophic failure to regulate surveillance trade - Amnesty International](#)

capabilities for telecommunications operators with its MENA office located in Amman; and the Israeli company Rayzone Group. <sup>30</sup>

### 4.3. Public Responses

The use of digital surveillance technology in Jordan has faced significant criticism from both local and international civil society organizations. In response to one investigation in Jordan, United Nations Special Rapporteur on Human Rights Defenders Mary Lawlor urged Jordan to uphold the rights to privacy and freedom of expression, citing its ratification of the International Covenant on Civil and Political Rights (ICCPR). <sup>31</sup>

In April 2023, a Jordanian member of parliament requested that the government's response to his inquiry about Pegasus spying on Jordanian phones include input from the National Cybersecurity Center. He highlighted that the government's response did not address reports documenting the targeting of Jordanian political figures and human rights defenders by Pegasus. The Minister of Interior replied that no formal complaints about such targeted surveillance had been filed by the individuals mentioned in the reports and asserted that there was no coordination or involvement between the Ministry of Interior and the spyware vendors referenced. <sup>32 33</sup>

---

<sup>30</sup> [Surveillance Watch](#)

<sup>31</sup> <https://x.com/MaryLawlorhrds/status/1753012751880851943>

<sup>32</sup> [حو 24 : مشوقة بسأل عن برنامج التحسس بيغاسوس .. ووزير الداخلية : لم تُقدم شكاوى للجهات المختصة](#)

<sup>33</sup> [مهم للأردنيين... قرارات حكومية جديدة](#)

## 5. Impact on Human Rights Defenders

### 5.1. Legal Consequences

Human rights defenders face dire legal consequences for legitimate forms of expression online. Human rights defenders in Jordan face administrative detention, long court trials often on dubious charges, which result in large fines and months-long prison sentences.

According to social media platforms' transparency reports, the Jordanian government commonly requests data from social media platforms for details about user accounts. In Meta's latest report, covering the months of July to December 2023, Jordanian authorities requested data about 1,052 user accounts and in the six months prior to that, it requested data on 1,247 accounts. <sup>34</sup>

Surveillance on social media platforms – or “online patrolling” – has indeed increased the rate of human rights defenders identified and summoned by authorities. In the last 10 months alone, local and international human organizations monitored the detention of thousands of pro-Palestine activists. <sup>35</sup>

In October 2023, Anas al-Jamal, an activist and member of the now forcibly dissolved Partnership and Salvation Party, was prosecuted and detained for three months under Article 24 of the 2023 Cybercrime Law. His detention was in response to three tweets he posted during that month, and he was subsequently fined approximately \$7,000. Al-Jamal had previously faced legal troubles in May 2022, when he was detained after being prosecuted under Article 118 of the penal code, which criminalizes actions that disturb relations with a friendly country. This earlier prosecution was triggered by a tweet in which al-Jamal criticized a meeting between Egyptian, Emirati, and Israeli leaders. <sup>36</sup>

In December 2023, Ayman Sanduka, an activist, teacher, and secretary of the Partnership and Salvation Party, was arrested following a Facebook post in which he addressed the King of Jordan and criticized the country's diplomatic relations with Israel. He was charged under Article 149 of the Penal Code by a military court for “incitement to oppose the political regime.” <sup>37</sup>

In February 2024, lawyer and human rights defender Motaz Awwad was called in for questioning by the cybercrime unit and subsequently detained following tweets he had written in support of Palestine and critical of Jordanian authorities' trade relations with Israel. <sup>38</sup>

---

<sup>34</sup> [Government Requests for User Data | Transparency Center](#)

<sup>35</sup> [State of Privacy Jordan](#)

<sup>36</sup> [Jordan: Arrests, Harassment of Pro-Palestine Protesters | Human Rights Watch](#)

<sup>37</sup> [Jordan: Political Activist Facing Trial Before Military Court for Facebook Post: Ayman Sanduka - Amnesty International](#)

<sup>38</sup> [Jordan's new Cybercrimes Law stifling freedom of expression one year on](#)

In March 2024, security forces administratively detained photojournalist Sherbel Dissi, also known as Ahmad Mohsen, while he was covering protests near the Israeli embassy in Amman for the independent media outlet 7iber.<sup>39</sup> During the same month, journalist Khair Eddin Aljabri was detained under Article 17 of the 2023 Cybercrime Law after sharing a news video online.<sup>40</sup>

Police forces arrested Fatima Shubailat from a supermarket in Amman on 17 April 2024. Fatima's arrest came against the backdrop of a video clip filmed by an unidentified individual and then circulated widely on social media platforms, in which Fatima appears, on March 30th, in a demonstration near the Israeli embassy in Amman in protest against Israel's crimes in the Gaza Strip and its siege of Al-Shifa Hospital. The video shows Fatima shouting at police saying "You are Jordanians? You are Americans, Zionists." According to her family, the video was edited to only show that clip and failed to show police assaulting Fatima, which they claim sparked Fatima's response.<sup>41</sup>

In April 2024, activist Khalid Al-Natour was detained twice since October 7th for his online posts expressing support for Gaza.<sup>42</sup> Two months later, in June 2024, journalist Hiba Abu Taha was sentenced to one year in prison for an article she had published in April 2024, which was critical of Jordan for intercepting Iranian missiles headed to Israel.<sup>43 44</sup>

Finally, in July 2024, activist and journalist Ahmad Hasan al-Zoubi was detained following the enforcement of a one-year prison sentence issued in mid-2023. Al-Zoubi's conviction was based on an online post he had written criticizing the country's policy of raising fuel prices in December 2022.<sup>45</sup>

---

<sup>39</sup> [CPJ calls on Jordan to free photojournalist Ahmad Mohsen - Committee to Protect Journalists](#)

<sup>40</sup> [Jordanian reporter gets one year in prison under draconian new cybercrime law | RSF](#)

<sup>41</sup> [Jordan's new Cybercrimes Law stifling freedom of expression one year on](#)

<sup>42</sup> [Detention of popular activist Khaled Al-Natour reflects Jordanian government's policy of systematic abuse](#)

<sup>43</sup> [Palestinian-Jordanian journalist Hiba Abu Taha sentenced to one year in prison](#)

<sup>44</sup> [Jordan's new Cybercrimes Law stifling freedom of expression one year on](#)

<sup>45</sup> [Jordan: Imprisonment of journalist Ahmad Al Zoubi is arbitrary, reinforces policy of suppression](#)

## 5.2. Behavioral Impact

The government's repressive measures, broad surveillance of human rights defenders, and use of ambiguous legislation such as the Cybercrime Law have created a wide chilling effect across the country's civic space.

As a result of rampant digital surveillance and its tangible negative consequences, self-censorship has duly increased.<sup>46</sup> This contributes to the fact that Jordanians have a long-standing belief that "someone is listening in" on their communications.<sup>47</sup>

---

46 [حرية الصحافة في الأردن بين رقابة السلطة والرقابة الذاتية | معهد الجزيرة للإعلام](#)

47 [A glimpse into the perception of "digital privacy" in Jordan - 7iber | حبر](#)

# 6. Recommendations

Over the years, civil society has repeatedly made recommendations to the government of Jordan regarding its surveillance and harassment of human rights defenders. This section seeks to reiterate these key recommendations, emphasizing the need for reforms that safeguard the rights to privacy, free expression, and peaceful assembly.

## Recommendations to the government of Jordan

- The Jordanian government must allow an independent investigation into the use of spyware against its citizens and residents.
- The government must establish a clear path to accountability and remedy for victims of targeted surveillance.
- Jordan must uphold its constitution and fulfill its obligations under the International Covenant on Civil and Political Rights (ICCPR).
- The Cybercrime Law must be repealed, and the ongoing intimidation campaign against human rights defenders must cease.

Furthermore, this report seeks to provide additional recommendations to third parties and human rights defenders to enhance efforts in countering surveillance and mitigating its effects.

## Recommendations to technology vendors and social media companies

- **Harden device security:** by allowing users to disable features commonly used as attack vectors by sophisticated spyware, such as a feature like Apple's Lockdown Mode,
- **Standardize privacy and security features across operating systems:** including the ability to disable control panels from lock screen, require a pin code to turn off a device, enable multiple user profiles on devices, and more.
- **Transparency on targeting of human rights defenders:** social media platforms must increase their transparency about government requests for user data, especially data of accounts belonging to human rights defenders and members of civil society.
- **Enable remote account disabling:** facilitate the ability to remotely disable social media accounts in case of the detention of a human rights defender.
- **Improve privacy and security features** within apps by streamlining options such as two-factor authentication, password changes, login alerts, and account recovery.

## Recommendations to human rights defenders

- 1. Update regularly:** Ensure that your applications, browsers, and operating systems are updated as soon as updates are made available.
- 2. Enable Lockdown Mode on Apple devices:** This feature restricts certain functions commonly exploited by spyware, enhancing protection against sophisticated attacks.
- 3. Restart your devices frequently** to disrupt potential attacks.
- 4. Use disappearing messages** for sensitive conversations.
- 5. Minimize data stored on devices** and consider keeping it offline or in a secure cloud.
- 6. Cover device cameras**, especially front-facing ones.
- 7. Use a secure VPN or proxy** to protect your internet connection and reduce the risk of “network injection” attacks, a common method for compromising devices.
- 8. Communicate securely with colleagues** and sources by using secure apps like Signal and WhatsApp. Enable features like Signal’s “Relay Call” and WhatsApp’s “Protect IP” for additional protection.
- 9. Consult experts on counter-surveillance** and have devices tested for advanced malware or spyware.

## 7. Conclusion

In conclusion, this report sheds light on the escalating state surveillance and the state-sponsored harassment and intimidation campaigns faced by human rights defenders, journalists, and civil society actors in Jordan.

The extensive use of surveillance technologies and the expanding surveillance capabilities of the Jordanian state, coupled with a complex array of restrictive laws that enable surveillance and censorship, are directly linked to the erosion of civic space in Jordan and have severely impacted privacy, free expression, and peaceful assembly.

These practices not only undermine individual freedoms but also hinder the vital work of civil society. Addressing these issues is crucial for upholding Jordan's international human rights obligations.

The report's recommendations underscore the need for independent investigations into state-sponsored use of targeted surveillance technologies, the establishment of oversight and accountability mechanisms, and the immediate repeal of oppressive laws. It also recognizes the responsibility of technology vendors and social media companies to improve the privacy and security of individuals, and encourages human rights defenders to adopt certain digital security practices.

In light of little reporting on the matter, the report encourages immediate and coordinated action from both national and international stakeholders in order to condemn Jordan's oppressive reality and create the political incentives needed to move towards fostering an open environment for civil society in the country.