



مؤسسة الحرية الرأي والتعبير وحقوق الإنسان
El Hak Foundation for Freedom of
Expression and Human Rights

AHRI

African
Human Rights
Index



RIGHTS | DIGNITY | JUSTICE

DIGITAL SURVEILLANCE AND THE RISKS OF ARBITRARY ARREST AND TORTURE

**El Hak Foundation for Freedom of Expression
and Human Rights**

◆ The African Institution for Human Rights ◆



www.elhak.org



info@elhak.org



Facebook: [elhak02](https://www.facebook.com/elhak02)



X: [@elhakcenter](https://twitter.com/elhakcenter)



26 July Street – In front of the High Court of Justice – Cairo, Egypt

DIGITAL SURVEILLANCE AND THE RISKS OF ARBITRARY DETENTION AND TORTURE IN AFRICA

An Analytical Report on the Findings of the 2026 African Civil Society Survey

El Hak Foundation for Freedom of Expression and Human Rights (EFHR)

African Human Rights Index (AHRI) Programme

September 2026

Foreword

This report builds on the work of the El Hak Foundation for Freedom of Expression and Human Rights in examining the growing relationship between digital surveillance, arbitrary detention, and the risks of torture and ill-treatment in Africa. It also reflects the Foundation's broader effort to develop research tools capable of capturing the new challenges that technology poses to human rights protection systems.

This work began while the Foundation was preparing a research paper addressed to the Committee for the Prevention of Torture in Africa, a special mechanism of the African Commission on Human and Peoples' Rights, in response to its 2026 call for contributions on "Torture and Digital Surveillance in Africa."

During the preparation of that paper, it became clear that the issue could not be adequately addressed through legal analysis alone or through a limited number of illustrative violations. Understanding the relationship between digital surveillance and torture requires direct engagement with the experiences of civil society organisations and other actors working on the ground across African countries.

Accordingly, through the African Human Rights Index (AHRI) Programme, El Hak Foundation launched an exploratory Africa-wide survey on digital surveillance and the risks of torture and ill-treatment. The survey sought to identify the principal forms of surveillance in use, the groups most exposed to targeting, the extent to which digital information moves from monitoring and surveillance into summons, arrest, detention, or interrogation, and the perceived effectiveness of legal and oversight frameworks, complaints mechanisms, and accountability processes.

The survey's preliminary findings were used as one source of evidence supporting the paper submitted to the Committee for the Prevention of Torture. However, the patterns, gaps, and intersections revealed by the responses—between digital surveillance, security action, and coercion—demonstrated that the material collected warranted broader and more detailed analysis beyond the scope and requirements of the shorter paper submitted to the Committee.

This report therefore represents the second stage of that research process.

It does not reproduce the earlier paper. Rather, it provides an independent and expanded analysis of the survey findings by presenting data, statistics, and charts; examining each thematic area of the questionnaire; and exploring the relationship between the existence of legal safeguards and the effectiveness of implementation, oversight, and practical outcomes.

The report also draws on the diagnostic methodology developed by the Foundation under the African Human Rights Index, which distinguishes between:

- legal and institutional structures;
- implementation and oversight; and
- actual outcomes.

This approach seeks to move beyond the conventional question of whether a State has a law regulating surveillance or protecting data, towards a more fundamental question:

Do these safeguards work in practice when surveillance data moves from the digital sphere into the security sphere? Can they prevent surveillance from becoming a means of targeting, arrest, coercion, and ill-treatment?

Given the nature and size of the sample, this report does not claim to provide a comprehensive statistical measurement of digital surveillance across Africa, nor does it rank countries or make generalised judgments about them. Instead, it offers an exploratory reading grounded in participants' field experience, helping to identify recurring patterns, protection gaps, and issues that warrant further research, investigation, and follow-up.

One of the most important lessons emerging from this work is that technological development requires the torture-prevention system to evolve as well.

In many cases, the chain of risk may begin before the moment of arrest, through the identification of a person, their location, or their network of relationships. It may then continue through the seizure of devices, extraction of data, and use of that data during interrogation or as a means of pressure against the person or those around them.

Digital surveillance can therefore no longer be treated solely as a matter of privacy or freedom of expression. It is increasingly part of the wider discussion on preventing arbitrary detention, torture and ill-treatment, and ensuring accountability for violations.

We hope this report contributes to a broader African discussion on this relationship, provides a basis for developing more precise monitoring and measurement tools, strengthens cooperation between civil society organisations and national and regional mechanisms, and supports the further development of the African Human Rights Index in future cycles.

Shady Amin

Cairo, 1 September 2026

Table of Contents

Report Methodology

Executive Summary

- 1. Scope of the Report and Analytical Methodology**
- 2. Who Participated in the Survey?**
- 3. Reported Patterns of Digital Surveillance**
- 4. Targeted Groups and Level of Prevalence**
- 5. From Surveillance to Security and Judicial Action**
- 6. Use of Digital Data and Coercion During Investigation**
- 7. The Link to Torture and Ill-Treatment**
- 8. Legal Framework, Oversight and Accountability**
- 9. Institutional Responsibility and Reform Priorities**
- 10. Strength of Documentation and Evidence Provided**
- 11. The Implementation Gap: An Integrated Reading of the Findings**
- 12. Sensitivity Analysis and Study Limitations**
- 13. Key Conclusions**
- 14. Recommendations**

Annex: Summary Table of Survey Findings

Report Methodology

This report is based on an analysis of the findings of the African survey on digital surveillance and the risks of torture and ill-treatment conducted by El Hak Foundation for Freedom of Expression and Human Rights (EFHR) under the African Human Rights Index (AHRI) Programme. The survey aimed to explore the experiences and assessments of civil society organisations and experts working on human rights, digital rights, and torture prevention in a number of African countries.

The questionnaire was designed as an exploratory research instrument intended to identify patterns, risks, and institutional gaps that merit further research and documentation. It was not designed as a statistically representative survey of the African continent or as a basis for statistical generalisation across all African States.

1. Number of Responses and Published Sample

The survey received 14 unique responses.

13 responses agreed to participate in the research. However, one of those responses expressly requested that its data be used “for internal purposes only”; it was therefore excluded from all figures, percentages, and charts published in this report, in accordance with the participant’s choice and the data-use conditions they specified.

Accordingly, the published findings in this report are based on:

12 publishable responses from 7 African countries.

The distinction between responses received and responses eligible for publication forms part of the ethical safeguards adopted by the Foundation in processing the survey data.

2. Nature of the Sample

The survey used purposive, non-probability sampling and was directed to civil society organisations, experts, and institutions working in, or possessing experience in, one or more of the following fields:

- human rights and civil and political liberties;
- digital rights and privacy;
- freedom of expression and journalists’ rights;
- protection of human rights defenders;
- legal assistance and monitoring of detention conditions;
- prevention of torture and ill-treatment;
- technology and digital security.

The report’s findings therefore reflect the experiences and assessments of the organisations and individuals participating in the survey. The percentages cited should not be interpreted as prevalence rates for Africa as a whole or for the country from which a response originated.

3. Data Processing and Cleaning

Before analysis, responses underwent a review and data-cleaning process that included:

- removing duplicate responses;
- verifying consent to participate and to use the data;
- excluding responses that did not permit publication of their findings;
- avoiding the consolidation of variables or categories that were not sufficiently equivalent to allow methodologically sound comparison.

4. Analytical Approach

The report relies primarily on descriptive data analysis, including:

- calculating the number and distribution of responses to each question;
- calculating percentages using the total number of valid responses for each variable as the denominator;
- treating each option in multiple-choice questions as a separate indicator of the pattern identified by the participant;

- comparing selected variables relating to the legal framework, oversight, and complaints mechanisms with reported outcomes concerning arrest, detention, interrogation, and coercion.

The report also uses selected cross-tabulations and exploratory comparisons to examine whether the presence of a legal framework or oversight mechanism is associated, within the sample, with the reduction or persistence of certain practical risks.

These comparisons do not constitute causal statistical tests and cannot establish that a particular factor caused a particular outcome. They are used solely to identify possible gaps between the legal framework, implementation, and practical outcomes.

5. Implementation-Gap Analytical Framework

The report draws on the diagnostic approach used by the African Human Rights Index (AHRI), which distinguishes between three interrelated levels:

Structural dimension: The existence of laws, institutions, and formal safeguards regulating digital surveillance and protecting privacy and related rights.

Implementation dimension: The effectiveness of authorisation, oversight, complaints, investigation, institutional independence, and access to evidence and technical records.

Outcome dimension: Whether surveillance or digital data is in practice associated with targeting, arrest, detention, interrogation, or coercion, and whether violations are followed by investigation, accountability, or remedy.

This framework makes it possible to move from the question “Does a legal rule exist?” to a more important human rights question:

“Does that rule work in practice to prevent violations and protect individuals when it is applied?”

6. Ethical Considerations and Participant Protection

The analysis respected the level of disclosure selected by each participant.

Data that participants restricted to internal use were not included in published figures or charts. The report also does not publish contact details or information that could unnecessarily identify individual participants.

This approach seeks to balance the research value of the information with the principle of do no harm and the protection of information sources.

7. Limitations of the Report

The findings should be read in light of several methodological limitations, notably:

- the limited sample size;
- the unequal distribution of responses across countries;
- the voluntary and non-probability nature of participation;
- the possibility of over-representation of organisations with a direct interest in, or experience of, digital surveillance;
- the difficulty of independently verifying all facts reported by participants;
- the covert nature of some surveillance operations, which may make them extremely difficult to detect or prove;
- the fact that temporal sequence between surveillance and arrest or detention cannot, by itself, be treated as sufficient evidence of causation.

The findings should therefore be treated as exploratory evidence of patterns, risks, and gaps that warrant further research, documentation, and investigation, rather than as a definitive measurement of the scale of digital surveillance across the African continent.

The principal value of the survey lies in its ability to reveal recurring patterns, identify questions that should feature more prominently in the work of torture-prevention mechanisms and digital-surveillance oversight bodies, and provide an initial basis for developing broader measurement tools in future phases of the African Human Rights Index Programme.

Executive Summary

The exploratory survey reveals a coherent pattern in participants’ experience: digital surveillance is not understood solely as a privacy or data-protection issue. In a significant number of responses, it appears as part of a chain extending to summons, arrest and detention; the use of data during investigation; coercion to unlock devices or accounts; and, in some cases, torture, ill-treatment, or severe psychological pressure.

Key Indicator	Finding
Publishable responses	12
African countries	7
Observed security/judicial action following surveillance	83.3%
Reported direct use of data in investigations	75.0%
Identified human rights defenders as a targeted group	83.3%
Reported a documented/likely/indicative link with torture	75.0%
Reported a clear or partial legal framework	75.0%
Viewed the complaints body as independent and effective	18.2%

The most significant finding is not merely the prevalence of different forms of surveillance, but the discrepancy between the existence of legal or institutional safeguards on the one hand and weak complaint and remedy pathways, alongside the persistence of reported adverse outcomes, on the other. In the published sample, 9 of 12 respondents reported a clear or partial legal framework, and 6 of 12 stated that judicial authorisation was required in all cases. Yet only 2 of the 11 respondents who answered the complaints question considered that an independent and effective complaints body genuinely existed.

In terms of outcomes, 10 of 12 respondents reported at least one case in which digital surveillance was followed by security or judicial action, and 9 of 12 reported direct use of digital information during investigation or interrogation. Seven of 12 described the link between surveillance and torture or ill-treatment as either directly documented or strongly likely; this rises to 9 of 12 when responses indicating incomplete signs are included.

These figures do not establish causation between surveillance and torture in every case, nor do they permit statistical generalisation across Africa. They do, however, provide exploratory evidence of a risk pathway that requires further documentation: digital surveillance, followed by security activation, then use of data during investigation, with the possible emergence of digital or physical coercion at later stages.

1. Scope of the Report and Analytical Methodology

1.1 Data Source and Published Sample

The survey was conducted online in Arabic and English between 8 and 22 August 2026. It targeted human rights and digital rights organisations, legal aid centres, national institutions, preventive mechanisms, researchers, and experts. Fourteen unique responses were received. One response was excluded because the respondent did not consent to participation. A second response was excluded from the published report despite consenting to the research because the respondent expressly restricted use to “internal use only.” The published sample therefore consists of 12 responses from 7 countries.

1.2 Analytical Rules

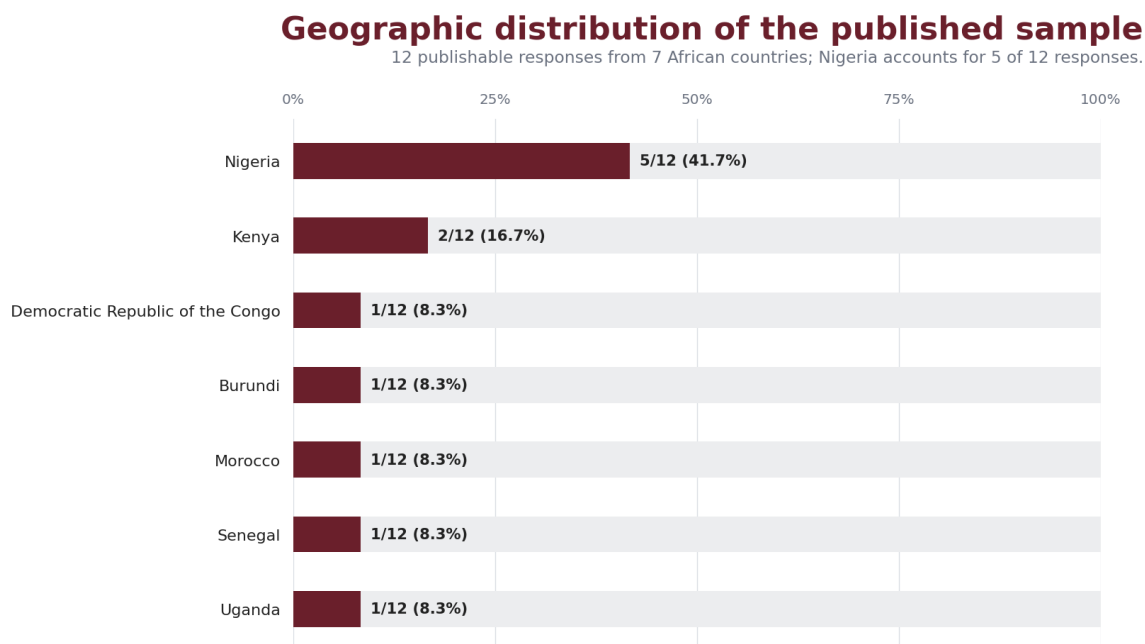
- The unit of analysis is the “response”, not the country; a single country may therefore have more than one participant.

- For multiple-choice questions, the percentage of participants selecting each category was calculated; totals therefore do not necessarily add up to 100%.
- Where a value is missing, the report uses the actual number of respondents to that question as the denominator and displays it alongside the result.
- No inferential tests or confidence intervals were used because the sample is purposive and non-probability.
- Organisation names, email addresses, and other identifying information were not published in the general analysis, even where some participants permitted attribution, in order to maintain a uniform level of protection.

2. Who Participated in the Survey?

The published sample covered seven countries. Nigeria accounts for 5 of the 12 responses (41.7%), and Kenya for 2 responses (16.7%). Burundi, the Democratic Republic of the Congo, Morocco, Senegal, and Uganda are represented by one response each. This distribution makes the findings relatively sensitive to Nigerian experience, an issue tested later through a separate analysis excluding Nigeria.

Figure 1 — Geographic distribution of the published sample.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

2.1 Type of Organisation

Eleven participants answered the question on organisation type. Because the question allowed more than one description for some respondents, “human rights organisation” was selected 7 times (63.6% of those who answered), while digital rights organisations, independent experts, and research or academic centres were each selected twice. One participant described the organisation as both a national human rights institution and a national preventive mechanism, reflecting diversity of backgrounds despite the small sample.

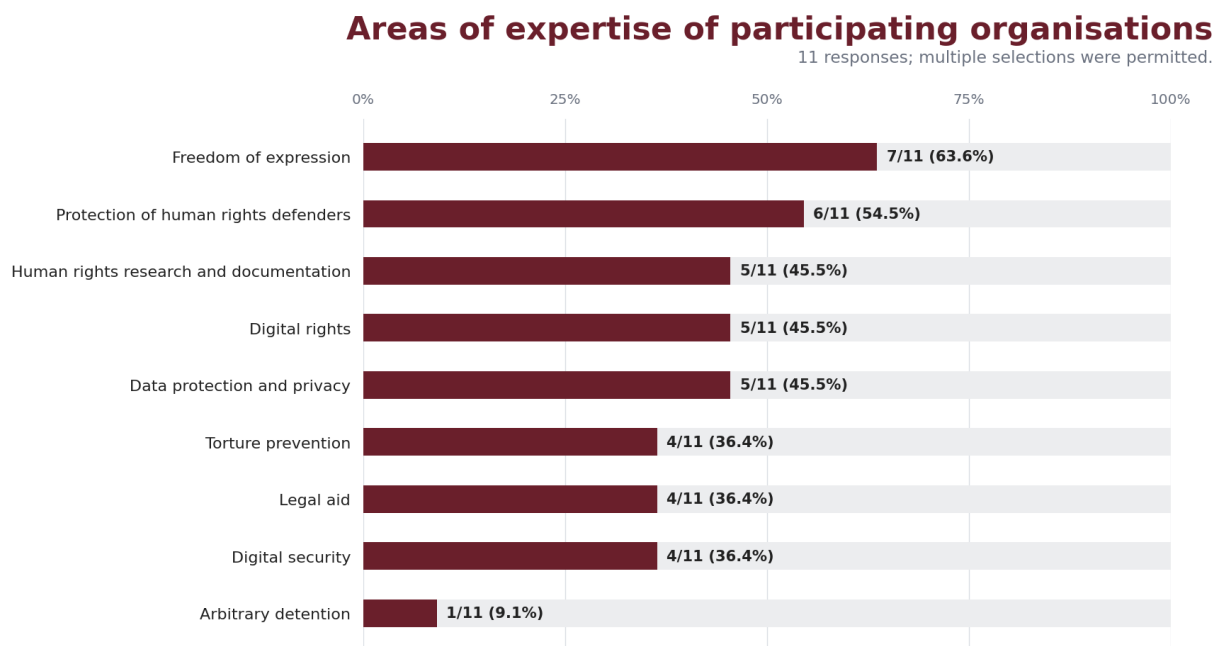
Type of organisation	Number of selections	Percentage of respondents
Human rights organisations	7	63.6%
Digital rights organisations	2	18.2%
Independent experts	2	18.2%

Research/academic centres	2	18.2%
Legal aid centres	1	9.1%
National human rights institution	1	9.1%
National preventive mechanism against torture	1	9.1%
Other	2	18.2%

2.2 Areas of Expertise

Participants' expertise is concentrated in freedom of expression, protection of human rights defenders, and digital rights—areas directly relevant to the survey topic. Of the 11 responses to this question, 7 selected freedom of expression (63.6%), 6 selected protection of human rights defenders (54.5%), and 5 each selected digital rights, research and documentation, and data protection and privacy (45.5% for each category). Four each selected torture prevention, legal aid, and digital security (36.4% for each). Four each selected torture prevention, legal aid, and digital security (36.4% for each).

Figure 2 — Areas of expertise of participating organisations.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

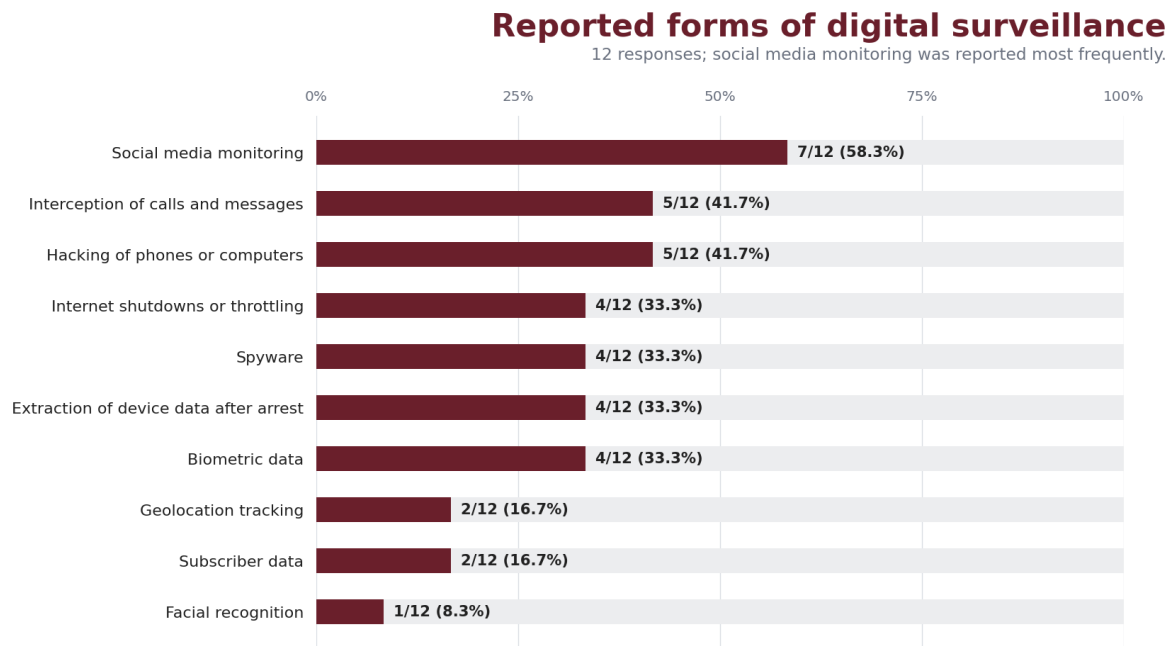
2.3 Disclosure Preferences

Among the 11 publishable responses that answered the disclosure-level question, 7 permitted the organisation and country to be named (63.6%), 2 requested country-only attribution (18.2%), and 2 chose fully anonymised use (18.2%). Irrespective of these preferences, the report uses aggregate presentation and does not publish participant identities.

3. Reported Patterns of Digital Surveillance

Social media monitoring was the most frequently reported practice, selected by 7 of 12 participants (58.3%). It was followed by interception of calls and messages and hacking of phones or computers, each selected by 5 participants (41.7%). Four participants each reported spyware, biometric data, extraction of device data after arrest, and internet shutdowns or throttling (33.3% for each category).

Figure 3 — Forms of digital surveillance observed by participants or reported to them through reliable information.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

These findings show that participants' understanding of "digital surveillance" is not limited to traditional interception of communications. It extends to a broader environment including social platforms, device hacking, biometric data, and extraction of phone contents after arrest. This breadth matters when assessing risk, because some tools operate before arrest to identify a target, while others are used during detention to obtain digital content.

4. Targeted Groups and Level of Prevalence

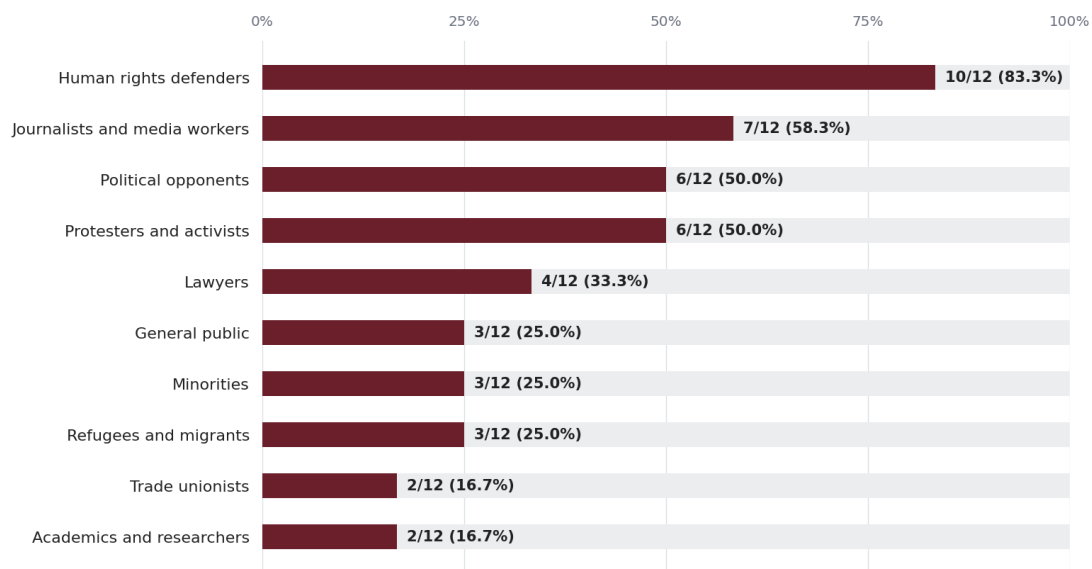
4.1 Human Rights Defenders Lead the Targeted Groups

Ten of 12 participants identified human rights defenders among the groups most exposed to digital surveillance, representing 83.3% of the published sample. Journalists and media workers ranked next, at 7 of 12 (58.3%), followed by political opponents and protesters or activists, at 6 of 12 for each category (50%). Lawyers were identified in 4 responses (33.3%).

Figure 4 — Groups participants considered most exposed to digital surveillance.

Groups considered most exposed to digital surveillance

12 responses; multiple selections were permitted.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

4.2 Three-Quarters of the Sample Rate Use as Moderate or Higher

When asked about the level of use of digital surveillance without adequate safeguards, 2 participants selected “very high” (16.7%), 4 selected “high” (33.3%), and 3 selected “moderate” (25%). Accordingly, 9 of 12 participants—75%—rated such use as moderate or higher. One participant selected “low”, one “very low”, and one “do not know”.

Assessment	Number	Percentage
Very high	2	16.7%
High	4	33.3%
Moderate	3	25.0%
Low	1	8.3%
Very low	1	8.3%
Do not know	1	8.3%

5. From Surveillance to Security and Judicial Action

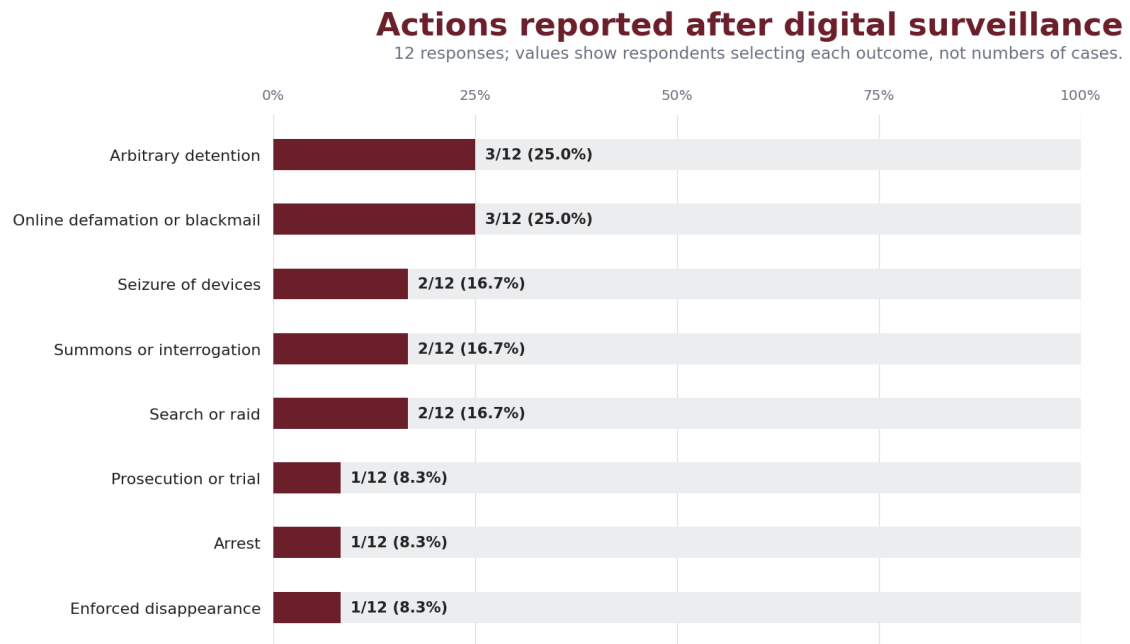
Eight participants reported observing “multiple cases” in which digital surveillance was followed by security or judicial action, while 2 reported one such case. In total, 10 of 12 participants (83.3%) reported at least one incident. One participant answered “no” and another “do not know”.

5.1 What Actions Followed Surveillance?

When the subsequent actions were disaggregated, the most frequently selected outcomes were arbitrary detention and online defamation or blackmail, each reported by 3 participants (25%). Seizure of devices, summons or interrogation, and search or raid were each reported by 2 participants (16.7% per category). Prosecution or trial, arrest, and enforced

disappearance were each selected once. These figures should not be read as “numbers of cases”; they represent the number of participants who selected each outcome.

Figure 5 — Actions participants reported as having followed digital surveillance.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

6. Use of Digital Data and Coercion During Investigation

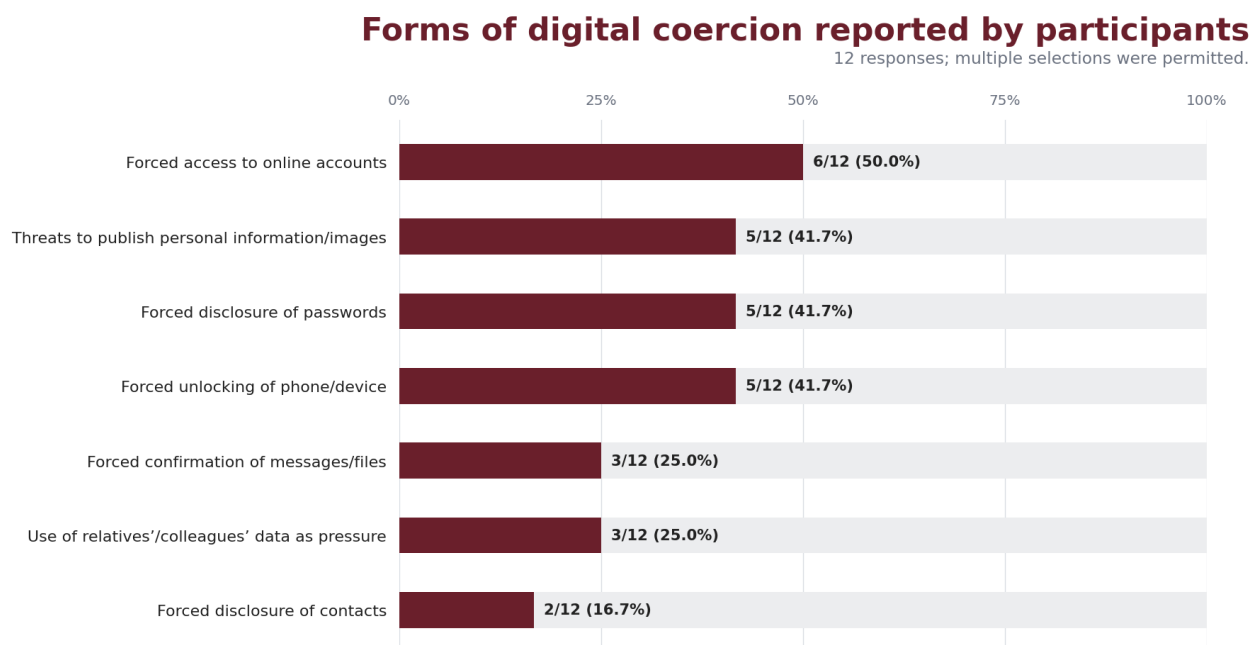
6.1 Direct Use of Data in Investigation

Nine of 12 participants (75%) directly reported the use of digital information or data during investigation or interrogation. This category includes all affirmative responses in both the Arabic and English versions, notwithstanding differences in how frequency was phrased. One additional participant indicated that there were “signs” of such use, while 2 selected “do not know”. The published sample recorded no explicit negative response to this question.

6.2 Digital Coercion Is Not Marginal in Reported Experience

The most frequently reported form of digital coercion was being forced to unlock online accounts, reported by 6 of 12 participants (50%). Disclosure of passwords and unlocking a phone or device were each reported in 5 responses (41.7%), while 5 participants also reported threats to publish personal information or images. Three participants reported being forced to confirm the authenticity of messages or files, 3 reported the use of relatives’ or colleagues’ data as a means of pressure, and 2 reported being forced to disclose contacts.

Figure 6 — Forms of digital coercion observed by participants.



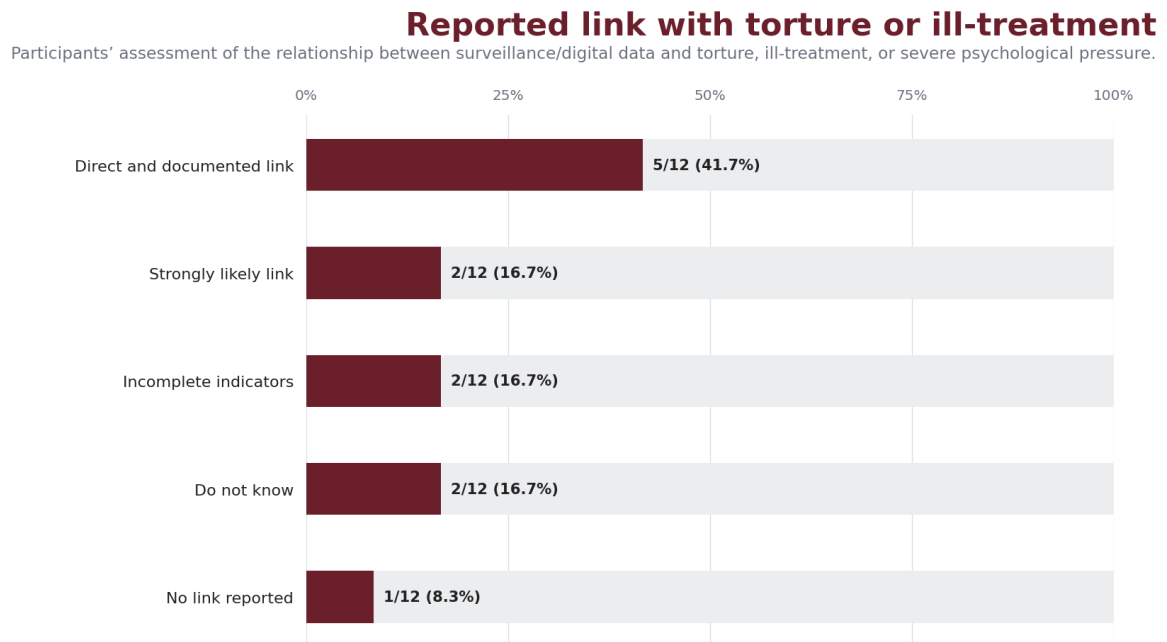
Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

These findings support the need to distinguish analytically between “extracting digital evidence” and “the manner in which it is obtained”. Data may be technical in form, but the circumstances in which a device or account is unlocked, or a password provided, may involve threats, pressure, or coercion. This is a central issue when assessing procedural integrity and rights during detention and investigation.

7. The Link to Torture and Ill-Treatment

Five of 12 participants described the relationship between surveillance or digital data and torture, ill-treatment, or severe psychological pressure as “direct and documented” (41.7%), while 2 described it as “strongly likely” (16.7%). Combined, these two categories account for 7 of 12 participants (58.3%). Two additional participants referred to “incomplete indicators”, raising the number who identified at least a possible link to 9 of 12 (75%). One participant answered in the negative and 2 indicated that they did not know.

Figure 7 — Participants' assessment of the link between digital surveillance and torture, ill-treatment, or severe psychological pressure.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

7.1 Risk Assessment

When asked more generally about the effect of digital surveillance on the risk of arbitrary arrest, detention, or torture, 8 of 12 participants (66.7%) considered that surveillance increased the risk to some degree: 2 to a very high degree, 3 to a high degree, 1 to a moderate degree, and 2 to a limited degree. Three participants considered that it did not increase the risk, while 1 selected “do not know”.

This finding differs from the preceding question: the first asks about a link observed in practical experience, whereas the second measures participants' assessment of risk. The two percentages should therefore not be combined into a single measure. Their proximity nevertheless reinforces the presence of a broad perception within the sample that surveillance may interact with risks of detention and coercion.

8. Legal Framework, Oversight and Accountability

8.1 Legal Frameworks Exist for a Majority of Respondents

Seven of 12 participants reported a “clear and comprehensive” legal framework (58.3%), while 2 described it as “partial or incomplete” (16.7%). Thus, 9 of 12 (75%) described the framework as either clear or partially present. One participant considered that no clear framework existed, one referred to scattered and unclear provisions, and one selected “do not know”.

8.2 Judicial Authorisation and Oversight

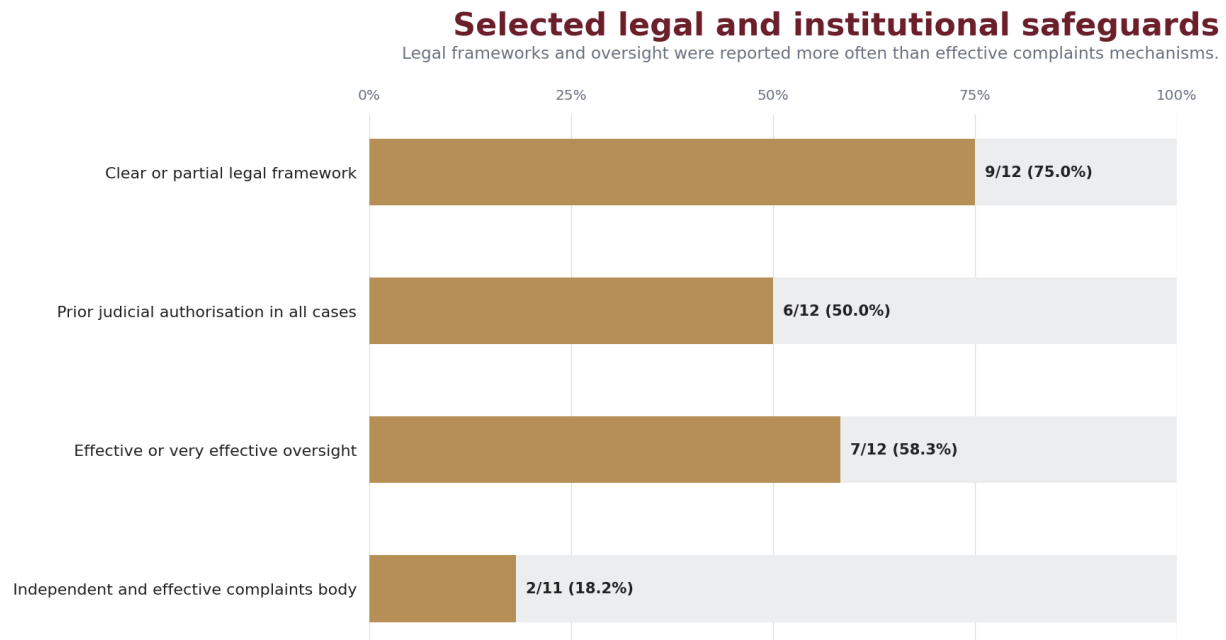
Regarding judicial authorisation, 6 of 12 participants stated that surveillance requires prior authorisation from an independent judicial authority “in all cases” (50%). Two referred to broad exceptions, 1 indicated that the requirement applies only to certain forms of surveillance, and 3 answered “do not know”.

As for judicial or independent oversight, 3 participants rated it “very effective” and 4 “effective”, giving a total of 7 of 12 (58.3%). One participant rated it moderate, 2 ineffective, 1 reported that no independent oversight existed, and 1 selected “do not know”.

8.3 Complaints Bodies Are the Weakest Link

Eleven participants answered the question on whether an independent and effective body exists to receive and investigate surveillance-related complaints. Only 2 considered that such a body exists and is effective (18.2% of respondents to the question), while 6 considered that a body exists but has limited effectiveness (54.5%), and 3 reported that no specialised or effective body exists (27.3%). Accordingly, 9 of 11 participants—81.8%—described the complaints mechanism as either of limited effectiveness or absent/ineffective.

Figure 8 — Comparison of selected legal and institutional safeguards as assessed by participants.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

The Absence of Law Is Not the Problem

The analysis strongly points to, and reinforces, the conclusion reached by the Foundation in its first African Human Rights Index report for 2025: the absence of law is not the principal problem. On the contrary, a majority of the sample reported the existence of a legal framework or some degree of oversight, while confidence in independent and effective complaints mechanisms was extremely low. This is the core of the “implementation gap” revealed by the survey.

9. Institutional Responsibility and Reform Priorities

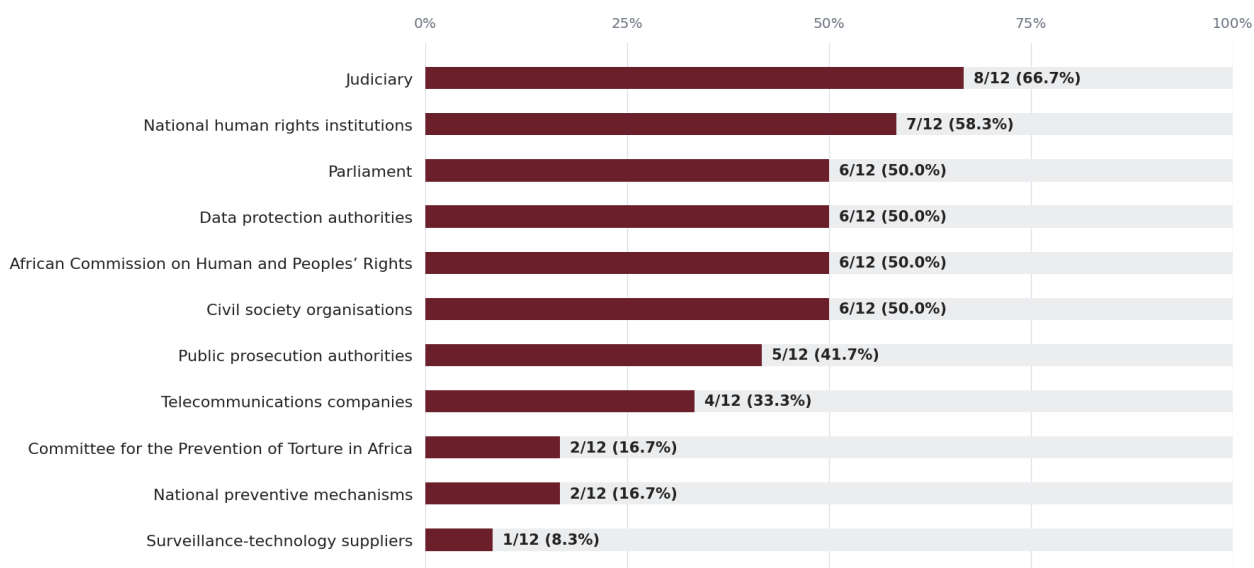
9.1 The Judiciary and National Institutions Lead the Bodies Whose Role Should Be Strengthened

Eight of 12 participants selected the judiciary as an institution that should assume a greater role in preventing misuse of surveillance (66.7%). National human rights institutions ranked second, selected by 7 of 12 (58.3%). Six of 12 selected each of parliament, data protection authorities, the African Commission on Human and Peoples’ Rights, and civil society organisations (50% per category). Five selected public prosecution authorities, 4 telecommunications companies, 2 each selected the Committee for the Prevention of Torture in Africa and national preventive mechanisms, and 1 selected surveillance-technology suppliers.

Figure 9 — Institutions participants believe should play a stronger role in preventing misuse of surveillance.

Institutions whose role participants believe should be strengthened

12 responses; multiple selections were permitted.



Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

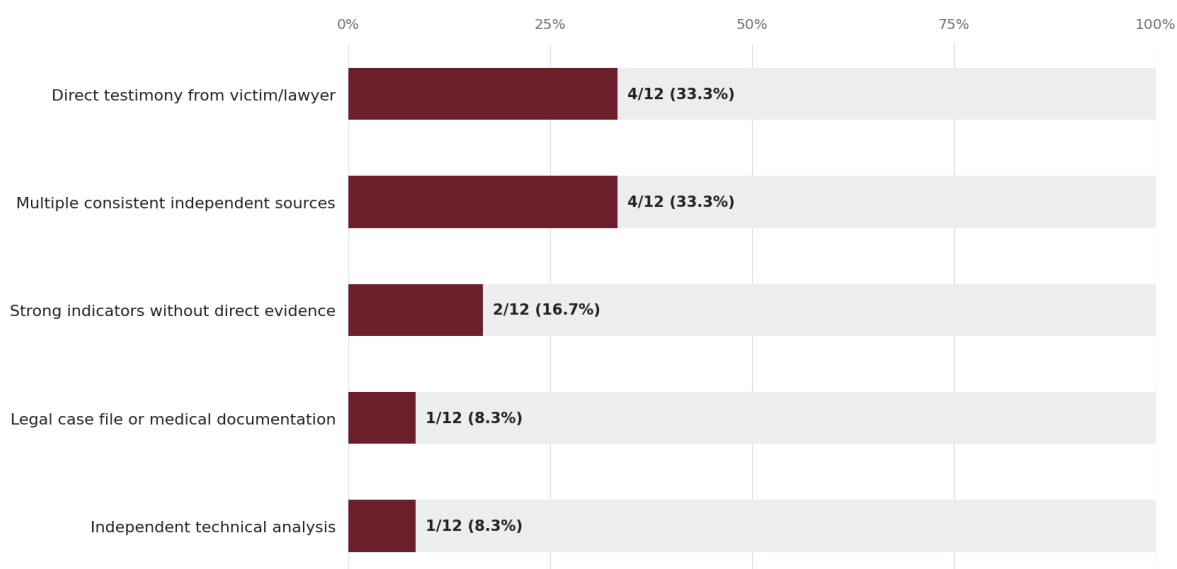
10. Strength of Documentation and Evidence Provided

The survey asked about the “highest available level” of documentation for the cases referenced; it did not ask whether the Foundation had independently verified every case. Four participants reported direct testimony from the victim or lawyer, 4 reported multiple independent and mutually consistent sources, 1 cited a legal case file or medical documentation, and 1 cited an independent technical analysis. The remaining 2 participants referred to strong indicators without direct evidence.

Figure 10 — Highest available level of case documentation, according to participants.

Highest available level of case documentation

12 responses; this reflects participants' descriptions and not independent verification by EFHR.



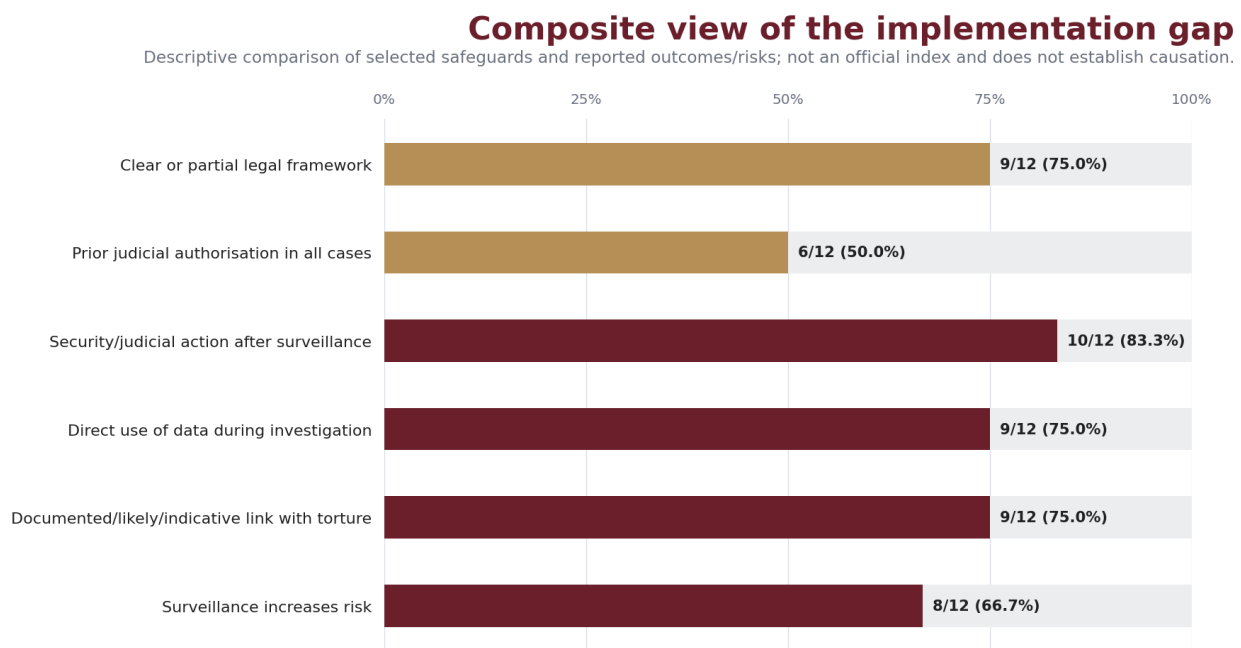
Source: El Hak Foundation survey on digital surveillance and torture risks in Africa, August 2026.

This finding increases the exploratory value of the data, but it does not transform the dataset into a verified case database. “Direct testimony” and “multiple sources” are descriptions supplied by participants of the highest level of documentation available to them.

11. The Implementation Gap: An Integrated Reading of the Findings

Reading the findings across three levels—legal structure, implementation and oversight, and outcomes—reveals a clear discrepancy. On one hand, 9 of 12 participants reported a clear or partial legal framework, 6 of 12 reported prior judicial authorisation in all cases, and 7 of 12 rated oversight as effective or very effective. On the other hand, 10 of 12 reported security or judicial action following surveillance, 9 of 12 reported direct use of data during investigation, and at least 9 of 12 reported either a documented link, a likely link, or indicators connecting surveillance with torture or ill-treatment. Only 2 of 11 considered the complaints body to be independent and effective.

Figure 11 — Descriptive comparison between selected safeguards and reported outcomes or risks. The figure does not constitute an official index or establish a causal relationship.



Source: EFHR analysis of survey findings. Gold represents legal/institutional safeguards; maroon represents reported outcomes or risks.

11.1 Cross-Analysis: The Existence of a Safeguard Does Not Mean the Absence of Adverse Outcomes

In an exploratory analysis within the sample itself, all 9 participants who reported a clear or partial legal framework also reported at least one case in which surveillance was followed by security or judicial action. All 9 likewise reported direct use of data during investigation, while 8 of 9 indicated either a direct relationship, a likely relationship, or indicators linking surveillance with torture or ill-treatment.

Similarly, all 6 participants who stated that judicial authorisation is required in all cases also reported subsequent security or judicial action and direct use of data during investigation; all 6 also indicated either a direct link, a likely link, or indicators relating to torture. Among the 7 participants who rated oversight as effective or very effective, all 7 reported subsequent action and direct use of data, and 6 indicated a possible link to torture or ill-treatment.

These relationships do not mean that law, judicial authorisation, or oversight “cause” violations, nor do they mean that such safeguards lack value. More plausibly, they indicate that measuring the existence of safeguards, or assessing them in general terms, is insufficient on its own to determine the level of actual protection. They may also reflect differing participant definitions of “effective oversight”, or the nature of a sample that is itself concentrated among organisations dealing with high-risk cases.

12. Sensitivity Analysis and Study Limitations

12.1 What Happens if Nigeria Is Excluded?

Because Nigeria accounts for 5 of the 12 responses, several core indicators were recalculated using the 7 participants from the remaining countries. The overall pattern persisted, although some percentages declined. Reports of security or judicial action following surveillance fell from 83.3% to 71.4%, direct use of data during investigation from 75% to 71.4%, and the documented/likely/indicative link with torture from 75% to 57.1%. The assessment that surveillance increases risk also declined from 66.7% to 57.1%.

Indicator	Published sample	After excluding Nigeria	Reading
Security/judicial action after surveillance	83.3% (10/12)	71.4% (5/7)	Pattern persists
Direct use of data during investigation	75.0% (9/12)	71.4% (5/7)	Relatively stable
Documented/likely/indicative link with torture	75.0% (9/12)	57.1% (4/7)	More sensitive to Nigeria's weight
Surveillance increases risk	66.7% (8/12)	57.1% (4/7)	Declines but remains a slight majority
Clear or partial legal framework	75.0% (9/12)	71.4% (5/7)	Relatively stable
Independent and effective complaints body	18.2% (2/11)	28.6% (2/7)	Remains limited

This test shows that Nigeria increases the intensity of some findings, particularly the reported link with torture, but does not create the pattern from scratch. A majority of respondents outside Nigeria also reported subsequent action and use of data during investigation. Nevertheless, the number remains extremely small and does not permit regional conclusions or statistically meaningful differences between countries.

12.2 Main Limitations

- The sample is purposive and non-probability and is not statistically representative of Africa.
- The findings rely on participant reports, and not every case was independently verified through technical or legal means.
- Temporal sequence between surveillance and arrest or torture does not, by itself, establish causation.

13. Key Conclusions

Conclusion 1

In the experience of most participants, digital surveillance is not a standalone privacy issue; it appears within a pathway that intersects with security action, investigation, and detention.

Conclusion 2

Human rights defenders, journalists, political opponents, and protesters are the groups most frequently identified by participants as being exposed to surveillance, reinforcing the link with freedom of expression and human rights work.

Conclusion 3

The use of digital data during investigation is widespread within the sample, and coercion to unlock accounts or devices or disclose passwords is not marginal in participant reports.

Conclusion 4

There are strong indications, among a majority of the sample, of a link between surveillance and torture, ill-treatment, or psychological pressure; however, the survey alone does not establish causation in every case.

Conclusion 5

The clearest institutional gap lies in complaints and remedy: the existence of laws, authorisation requirements, or oversight is not matched by a comparable level of effectiveness in complaints and investigation mechanisms.

Conclusion 6

The data support using a “structure – implementation – outcomes” approach in future studies, rather than measuring the existence of legislation alone.

Conclusion 7

The report is a starting point for deeper research based on documented country cases, not the end of the measurement process.

14. Recommendations

Policy and Prevention Recommendations

- Strengthen the independence and effectiveness of bodies receiving and investigating complaints concerning misuse of surveillance, including by enabling access to technical records and surveillance authorisation orders.
- Establish explicit safeguards against coercion to disclose passwords or unlock devices or accounts, and ensure scrutiny of the lawfulness and voluntariness of the acquisition of digital evidence.
- Strengthen oversight of the use of spyware, data-extraction tools, and biometric data, and avoid relying solely on formal judicial authorisation without subsequent oversight and effective remedy.
- Integrate digital risks into the work of national human rights institutions and national preventive mechanisms against torture, particularly when examining conditions of arrest and interrogation.
- Develop transparency and due-diligence obligations for telecommunications companies and surveillance-technology suppliers where there are foreseeable risks that their products may be used in human rights violations.
- Provide particular protection to journalists, human rights defenders, lawyers, and others whose digital data may expose networks of sources, clients, or human rights partners.

Annex: Summary Table of Survey Findings

Question / thematic area	Numerical summary
Consent to participate	13 of 14 unique responses consented; one non-consenting response was excluded.
Publication base	One consenting response that selected “internal use only” was excluded; n=12 published.
Countries	7 countries; Nigeria 5, Kenya 2, and one response from each remaining country.
Type of organisation	11 responses; human rights organisations were the most frequent (7/11).
Expertise	Freedom of expression 7/11; protection of defenders 6/11; digital rights, research, and data protection 5/11 each.
Forms of surveillance	Social media monitoring 7/12; interception of communications 5/12; device hacking 5/12.
Targeted groups	Human rights defenders 10/12; journalists 7/12; political opponents and protesters 6/12 each.
Level of prevalence	9/12 rated it moderate or higher.
Actions after surveillance	10/12 reported at least one case.
Use of data in investigation	9/12 direct reports; 1/12 indicators; 2/12 do not know.
Digital coercion	Unlocking accounts 6/12; disclosing passwords 5/12; unlocking devices 5/12; threats to publish information 5/12.

Link to torture	7/12 direct/strongly likely; 9/12 when incomplete indicators are included.
Increase in risk	8/12 consider that surveillance increases risk to some degree.
Legal framework	9/12 clear or partial.
Judicial authorisation	6/12 in all cases; 2/12 with broad exceptions; 1/12 for some forms; 3/12 do not know.
Oversight	7/12 effective or very effective.
Complaints body	2/11 effective; 6/11 limited; 3/11 no specialised/effective body.
Institutions whose role should be strengthened	Judiciary 8/12; national institutions 7/12; parliament, data protection authorities, African Commission, and civil society 6/12 each.
Level of documentation	10/12 direct testimony or independent/documentary/technical support; 2/12 strong indicators without direct evidence.

El Hak Foundation for Freedom of Expression and Human Rights
African Human Rights Index (AHRI) Programme
www.elhak.org | info@elhak.org