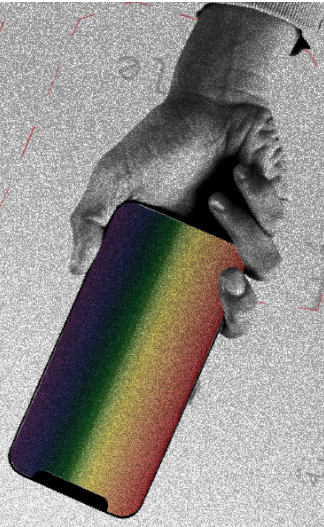
ARTICLE 19

Queer resistance to digital oppression



MENA's tech-enabled targeting of queer communities: An investigation

July 2024

Part II

In collaboration with the DeCenter

ARTICLE 19
72-82 Rosebery Ave
London EC1R 4RW
UK
www.article19.org

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices.

Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our nine regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on five key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
X: @article19org
Fb: facebook.com/article19org

Contents

Abbreviations

FATA	Iranian Cyber Police
LGBTQI+	Lesbian, gay, bisexual, transgender, queer, and intersex
MENA	Middle East and North Africa
NGO	Non-governmental organisation
PIN	Personal identification number
SMS	Short message service (text messaging)
UNHCR	United Nations High Commissioner for Refugees
VPN	Virtual private network

Acknowledgements

These acknowledgements are drafted by Afsaneh Rigot. Afsaneh is the creator, principal researcher, and coordinator of the project on the tech-facilitated harms against lesbian, gay, bisexual, transgender, queer, and intersex (LGBTQI+) communities in the Middle East and North Africa (MENA) and its reports, working alongside the LGBTQI+ community. She led this project as part of ARTICLE 19 from 2016 to 2023 and has continued as a consultant senior adviser and principal researcher for the reports while transitioning into new positions outside ARTICLE 19. This research was built out of her deep love and admiration for the MENA queer community and her belief in the vision for their better futures.

Afsaneh and the De|Center team continued to collaborate in the writing of these reports, and their analyses provided necessary tech methodology practices under Design From the Margins.

The list of those who supported this work is too long to fit into this section, but we deeply thank every person involved in the project. These include the following teams:

In **Algeria**, we would like to thank the Algerian team (who will remain anonymous for their safety). We especially thank them for the data they gathered and for conducting focus groups in a context that had not been covered before due to its great risk.

In **Egypt**, we thank the partnership and work of the Bedayaa organisation whose work and support have been pivotal throughout this project, especially for gathering data and lived experiences via interviews and focus groups from Egypt's queer community.

In **Iran**, we would like to thank our advisers and LGBTQI+ experts, but especially journalist and human rights defender Khosro Isfahani. Khosro conducted desktop research and in-depth interviews to gather vital insights from a particularly at-risk community.

In **Jordan**, we would like to thank Bin Amman (alias), Khalid Abdel-Hadi (editor-in-chief at *My Kali* magazine), and activist Hasan Kilani for their brilliant work in gathering context and conducting deep interviews in Jordan under increasing risks and difficulties.

In **Lebanon**, we would like to thank the many people that supported the work, especially researcher and sexual orientation, gender identity, and expression (SOGIE) expert Genwa Samhat, who was the lead coordinator and conducted deep interviews with some of the most marginalised community members, and Helem, an LGBTQI+ non-governmental organisation (NGO), for their pivotal support in conducting focus group discussions (with support from Sally Chamas) and gathering data for the surveys. We also thank the legal experts from Legal Agenda who provided invaluable legal and policy reviews and advice for this work.

In **Morocco**, we would like to thank Youba Darif and Roots Lab Morocco for their continuous and rich collaborations, impactful work, and leading data gathering in interviews and focus groups.

In **Sudan** we would like to thank Azza Nubi, Sam Adam, and Gamil for their deeply important work during one of the most painful periods of the country's history. They gathered contextual information and conducted deep interviews in a complex environment. Due to their meticulous work, we are able to present a small insight into the tremendous power of the Sudanese queer community, even during one of the worst humanitarian crises in modern history.

Finally, in **Tunisia**, we would like to thank Mawjoudin for their rich knowledge, interdisciplinary work, and support in this project, especially for gathering meaningful interviews and conducting focus groups.

We would also like to thank all the legal experts who provided reviews and insight for the complex legal labyrinths in each legal context. None of this would have been possible without the work of the community behind this report.

Further, we would like to thank our research and project assistants throughout the years: queer feminist expert Senda Ben Jebara; Ali Bousselmi, co-founder and executive director of Mawjoudin; and our Algeria expert, who will remain anonymous. They were a guiding light for this report and the main reason this project continued to function through all its complexities.

We would also like to thank our technical and international experts, many of whom have supported the work behind the scenes and attended our convenings to push for the implementation of the community's needs by tech companies. These include Kendra Albert, Mohammed Al-Maskati, Mahsa Alimardani, Sarah Aoun, Dia Kayyali, Moussa Saleh, and Apryl Williams.

We especially thank Nathan Freitas and the Guardian Project, Carrie Winfrey of Okthanks, and Norman Shamas, who were our technical experts co-leading the tech recommendations of these reports and many of its technical paths.

We also thank writer and editor Roja Heydarpour for her diligent, deeply attuned, and brilliant editing of texts of this project. We thank Manar Elharaké, the director of Astrum, for his excellent work coordinating the analysis of the thousands of complex survey data from many different dialects and languages and supporting the work to bring the findings to light. We thank our brilliant designer for the striking design work; as they are part of the community, they will remain anonymous. We thank Jessica Fjeld and Aymen Zaghdoudi for reviewing the report and their continuous support for the work.

Finally, we would also like to thank the numerous ARTICLE 19 teams and individuals who made this report possible, such as Maria Luisa Stasi who conducted our legal oversight, the ARTICLE 19 comms, editorial, and production team, and the Iran and MENA team.

This set of reports and the impact this work has had in the last eight years would not have been possible without the deep commitment, bravery, and genius of the LGBTQI+ community and experts on the ground fighting for better futures for all. This work is dedicated to them and their resistance. It is also dedicated to Palestine and the Palestinians, who, during the finalisation of this report, have been facing one of the most devastating and violent periods in modern history. Palestine might not be a focus of this report, but many of us learned the true meaning of living our truth, and living in resistance and resilience, from them.

Introduction

From 2019 to 2024 ARTICLE 19 worked with experts and non-governmental organisations (NGOs) in Algeria, Egypt, Iran, Jordan, Lebanon, Morocco, Sudan, and Tunisia to conduct interviews, hold focus group discussions, and run surveys. This is one of the largest research projects to date that investigates LGBTQI+ people and technology-facilitated harms in the region (and potentially globally). In this report – Part II of our three-part series – there is detailed analysis of in-depth, one-on-one interviews with **93 LGBTQI+ people and 5,000-plus online survey responses**, and summaries of **15 focus group discussions with 94 people in 6 countries**. Our work focused on the weaponisation of technology against the LGBTQI+ community, with emphasis on dating apps and social media platforms, as well as chat-based apps.

This research yielded this three-part report series in which ARTICLE 19 explores and investigates the technology-facilitated harms and abuses faced by the queer community in the Middle East and North Africa (MENA) in collaboration with the De|Center, with support from local experts in eight MENA countries and technical experts.

The ARTICLE 19 team has been leading work documenting how technology has been used to target the LGBTQI+ community in MENA since 2016, with a community of researchers, experts, and organisations in the region and internationally. We have worked with our experts to bring about major safety changes to platforms and apps which have translated into documented protection in times of arrests and abuse. This three-part series is the latest addition to the work, part of our mission to keep pushing for these changes and to continue to uplift the stories, experiences, and direct needs of the communities.

Due to the timing of the work, our findings show some of the most extreme dangers and contexts for the populations at large, with LGBTQI+ communities facing further compounding harms and abuses on the part of law enforcement and states, and military violence. We conducted the work during periods that included major uprisings, violent wars, coups, and increasing militarisation and occupation.

In this research we found harrowing and egregious reports of police and state violence against the LGBTQI+ community: **157 (25%) out of 641 people in our surveys reported**

experiencing physical abuse and violent harassment. This includes rape, physical and verbal violence, and humiliation and emotional torture. Among these experiences, there were **seven direct cases of rape by state-affiliated persons**.

In our interviews, **60 out of 93 (65%) people reported serious police violence and abuse**, and **all of our focus groups mentioned serious police violence and abuse. Every single sex worker, trans, and refugee participant experienced police abuse.**

The report also reveals the use and combination of police violence with violations of privacy and other human rights involving both new technology tools and traditional policing methods:

__45%__ of our survey respondents and interviewees had been arrested for their sexual orientation and/or gender identity – and __over 1 in 5__ had been arrested multiple times.

The breakdown of this shows that **out of 93 interviewees, 54 (58%) reported they had experienced arrests** of some sort. Similarly, **272 (43%) out of 641 respondents had experienced arrests**. In the **focus groups, at least three people in each in each country had experienced arrests**. Over **20%** of our respondents and participants had **experienced arrest multiple times**. These arrests include entrapment by police, on-street arrests, reports from other people to the police or security forces, or opportunistic arrests. Our multiply marginalised interviewees (trans people, sex workers, refugees) had experienced the highest rates of arrests and abuse.

In our surveys, **159 out of 641 (25%) respondents reported experiences of state/police entrapments**. We previously saw undocumented use of entrapment in cases in Lebanon. The most mentioned apps used for entrapment were Grindr, Tinder, Hornet, Sugar, WhosHere, Snapchat, Facebook, WhatsApp, and Instagram. In 53 cases, different entrapment-style luring was used by police only to extort money or sexual favours from people.

10 out of 54 (19%) interviewees who reported being arrested had **experienced app entrapment**. **A total of 23% of our survey and interview participants thus had experienced entrapment.**

Importantly, **12 out of 93 (13%) interviewees** directly reported such arrests as **linked to protests and 'morality' policing** in this research period, showing criminalisation and targeting of queer people during national uprisings, protests, and even war.

Our report shows extensive use by MENA authorities of device searches to verify (or leading to the verification of) queerness of an individual as well as for the use of digital evidence.

***47 out of 93** (50%) interviewees had experienced device searches in the **8 countries** studied.*

Nearly every interviewee who had had an altercation or interaction with the police and law enforcement in these cases had had their devices searched or attempted forced access to devices.

An emerging and major concern is the severe risks of new tech features in the name of preserving privacy, such as **biometrics**. The use of biometrics has added risks of physical violence and force.

***7 out of 93** (8%) interviewees had biometrics enabled on their devices, and all of them were forced to open their devices using the biometrics. In **5** cases, violence was used.*

In every case where our interviewees or participants were in custody and had biometrics enabled – such as Face ID or fingerprint unlocking features – they were forced to access their device and did not have the option to refuse or negotiate this demand. In **5 out of the 7 cases** (and thus the majority), **law enforcement used violence** against individuals to force the use of biometrics to open their devices.

In Sudan, all of the abuses and dangers that existed online and offline have been vastly exacerbated since the coup and the start of war. Our report provides further insight into these issues and abuses, including some that have been documented for the first time. This report provides the background documentation that feeds into our recommendations in Part III.

Methodology and how to understand our data

Research ethics and safety

ARTICLE 19 aimed to ensure continuing adherence to ethical procedures from the outset, and relative to each context, throughout the work. Although the research process was conducted in accordance with all required ethical standards, these ethics were not considered a goal, but rather guiding principles that governed the study from start to finish: from the initial design of research tools, through the conduct of the analysis, to the writing process and publication of the study.

To ensure no individuals or organisations are placed at risk due by its research, ARTICLE 19 continually checks with individuals and organisations to make sure that everything possible is done to minimise risk.

All personal identities relating to highlighted cases and stories are anonymised, and all efforts have been made to keep people's invisibility protected throughout the research. This means working closely with partners in each country – the partners themselves are credited by name only when they have provided us with permission to do so under their own security assessments. We used customised security methods for data retention and communications, working closely with digital security experts within our organisation and externally. In addition to these procedures and assessments, these methods were applied to our data collection and retention to ensure constant safety.

ARTICLE 19 will continue to encourage the use of holistic digital security practices as the work is published. The data of this project will be maintained securely (without public access due to the safety needs of those involved) for five years from the date of publication. After five years we will review whether more work will be done with the data of the research (based on the recommendation and advice of local teams and communities' representatives) or whether we will permanently and securely delete the data. Importantly, all participants in the research interviews were asked to provide informed consent and were also informed of their right to withdraw from the study at any stage.

Finally, close attention has been paid to how the research is presented to those who come, directly or indirectly, in contact with the study. This is an important aspect of any ethical approach to research which requires diligent attention and care. ARTICLE 19 worked with local partners to develop country-specific risk assessment for those engaged in the research. However, the assessment remains a live document throughout the whole process of research. Live risk assessment helps ARTICLE 19 and its implementing local partners to stay continuously alert to (any change in) the security conditions which may affect LGBTQI+ communities taking part in the research.

Interviews

To gain a deeper understanding of the experiences and abuses of the community, we conducted **93 in-depth interviews with LGBTQI+ people in 8 countries**. This manageable sample was identified and interviewed by our in-country experts and partners in each country based on the questions, outlines, and specifications provided by ARTICLE 19.

The interviewees were selected based on experiences of either arrests, abuse, or violence based on their gender and sexual identities, as well as their use of technologies. ARTICLE 19 wanted to maintain a heavy focus on the highly marginalised members of the LGBTQI+ community where possible: refugees, sex workers, and trans people.

The interviews were semi-structured with 35–40 questions curated by the ARTICLE 19 research team. Though ARTICLE 19 maintained the same structures – with the sections (1) demographics, (2) use of technology, (3) changes demanded from companies, and (4) technology-related human rights and abuse experiences – for all the interviews in each country, we worked with our local partners on the ground to ensure the questions were relevant and safe. As a result, each country made slight adjustments to ensure contextual understanding and limit unnecessary risk. Our questions were translated into each country's specific languages and dialects.

The design of the interview questions was informed by consultations with in-country experts and based on principal researcher Afsaneh Rigot's eight years of involvement in and work on the subject area.

To further ensure the safety and trust of our interviewees, the interviews were conducted by our research teams on the ground who held trusted relationships with the interviewees. Our local teams worked from interview standards and methodologies defined by ARTICLE 19.

In the findings, we redact any information that might cause further risk to or targeting of our interviewees. For safety, we have excluded some of the more sensitive interviews from the project based on the uniqueness of the cases and where we assess that the individuals are in a continued state of risk based on their cases, including if they have had ongoing legal cases against them brought by the state.

We conducted a total of 93 interviews between January 2021 and August 2023 (see Table 1). In Sudan, due to the extreme and devastating change that occurred after April 2023 and the outbreak of war, we conducted six supplementary interviews to obtain an understanding of the experiences of queer Sudanese people in their new context so that our recommendations also consider their needs.

Table 1: Breakdown of interviews

Country	Interview dates	No. of interviews
Algeria	July 2022	10
Egypt	March 2023	10
	July 2022	1
Iran	January 2021	13
	February 2021	1
Jordan	November 2022	10
Lebanon	September 2022	2
	November 2022	6
	March 2023	4
Morocco	March 2022	10
Tunisia	July 2022	10
Sudan	August 2022	10
	August 2023	6
Total		**93**

Due to concerns for the safety of the participants and the complexity of the subject matter, these interviews were analysed manually and individually by Afsaneh Rigot, the research lead of the project.

The interviews were recorded and then transcribed manually by trusted consultants: manual transcription was selected as the preferred method of transcription as auto-transcription tools lack the technical capacity to accurately transcribe content from sources that use non-Western scripts. They also have many data privacy issues. Several interviews were conducted through interpreters, and quotes derived from such interviews are based on interpreted content. Some variance was expected; clarifying follow-up questions were asked in instances of confusion or uncertainty.

Once the transcripts were finalised, the data was used as the basis for a manual coding process which is reflected in the structure of the report.

Surveys

In order to widen the pool of respondents and experiences, we used mixed-method and quantitative-light online surveys. These surveys contained around 40–45 questions.

ARTICLE 19 used two main methods:

ARTICLE 19's local partners distributed surveys through online and offline channels. In places without internet access, phone calls or in-person meetings were used.

Company platforms such as Grindr partnered with ARTICLE 19 and sent surveys to users as a pop-up notification.

All surveys were translated into each country's specific language or dialects with the support and review of our local country experts.

The surveys were sent out periodically between December 2020 and July 2023. The survey questions followed the same structure as our interview questions, with a further focus on technology changes and demands. The total number of surveys was 5,018, with 4,072 complete survey responses (see Table 2) and 946 incomplete surveys (these are cases where the respondents did not finish the full survey).

Table 2: Breakdown of survey responses

Country	No. of responses
Algeria	1,155
Egypt	1,228
Iran	62
Jordan	342
Lebanon	1,281
Morocco	492
Sudan	91
Tunisia	367
Total	**5,018**

The full findings of our survey are available on the project webpage.

Important note on result presentation

We provided the option for individuals to skip questions they did not want to answer in these large and mass-scale surveys due to the high-risk nature of this data gathering and to ensure our respondents' safety and autonomy. Thus, we analyse and outline the number of results based on **how many people responded to a particular question** or section and not the whole number of survey respondents.

In some countries such as Iran and Sudan, we gathered a lower number of responses due to the intense security risks, internet shutdowns, and layers of online censorship.

We consulted with digital technologists and local community experts about surveying platforms. The platform we landed on was selected after vetting the security practices, accessibility, and functionality in different languages, as well as the ability to access it in our many different countries (the platform's name is redacted as an extra precaution as we still maintain some data on the platform).

Due to the volume and number of the responses, it was impossible to manually review these results. The data was analysed by Manar El Harake, founder of Adstrum Management. The analysis involved a rigorous methodology that included manual translation of qualitative data from eight countries and detailed categorisation in two stages: comprehensive data validation using RStudio, and visualisation through interactive Power BI dashboards. The careful translation and categorisation addressed linguistic and cultural nuances, while the validation process confirmed the consistency of responses across various metrics. The resulting eight-page interactive dashboards facilitated an in-depth analysis. The data compilations were then reviewed manually between the research team (Afsaneh Rigot, the principal researcher) and Manar El Harake.

Much of the data has not been presented in this report and the dashboard due to the sheer volume and, in some cases, due to safety. (Some of our respondents provided very detailed descriptions of their abuse incidents, or tools used, and upon risk assessment, our teams decided that the safety protocols of this project required us to redact and remove these cases from our findings.)

Focus groups

Our final method to gain insight into these experiences and demands from the communities was through group discussion and focus groups. In groups, the setting was an important part of the community-building aspect of the project. Furthermore, there was an understanding that these experiences are not individualised processes, but systemic and deeply sowed into the community as a whole. These focus groups allowed for trust-building and the exchange of experiences, which led to a better understanding of the patterns of abuse, as well as the technology-based harm reduction changes wanted.

Participants could share their experiences with each other, highlight the patterns of needs or abuses, and also bond with one another, ensuring that the recounting of these abuses was not a lonely process. We worked with local organisations and expert researchers to conduct focus groups in **6 of the 8 focus countries**: Algeria, Egypt, Lebanon, Morocco, Sudan, and Tunisia. We did not conduct groups in Iran and Jordan due to security concerns. There were 15 focus groups in total with 94 participants (see Table 3).

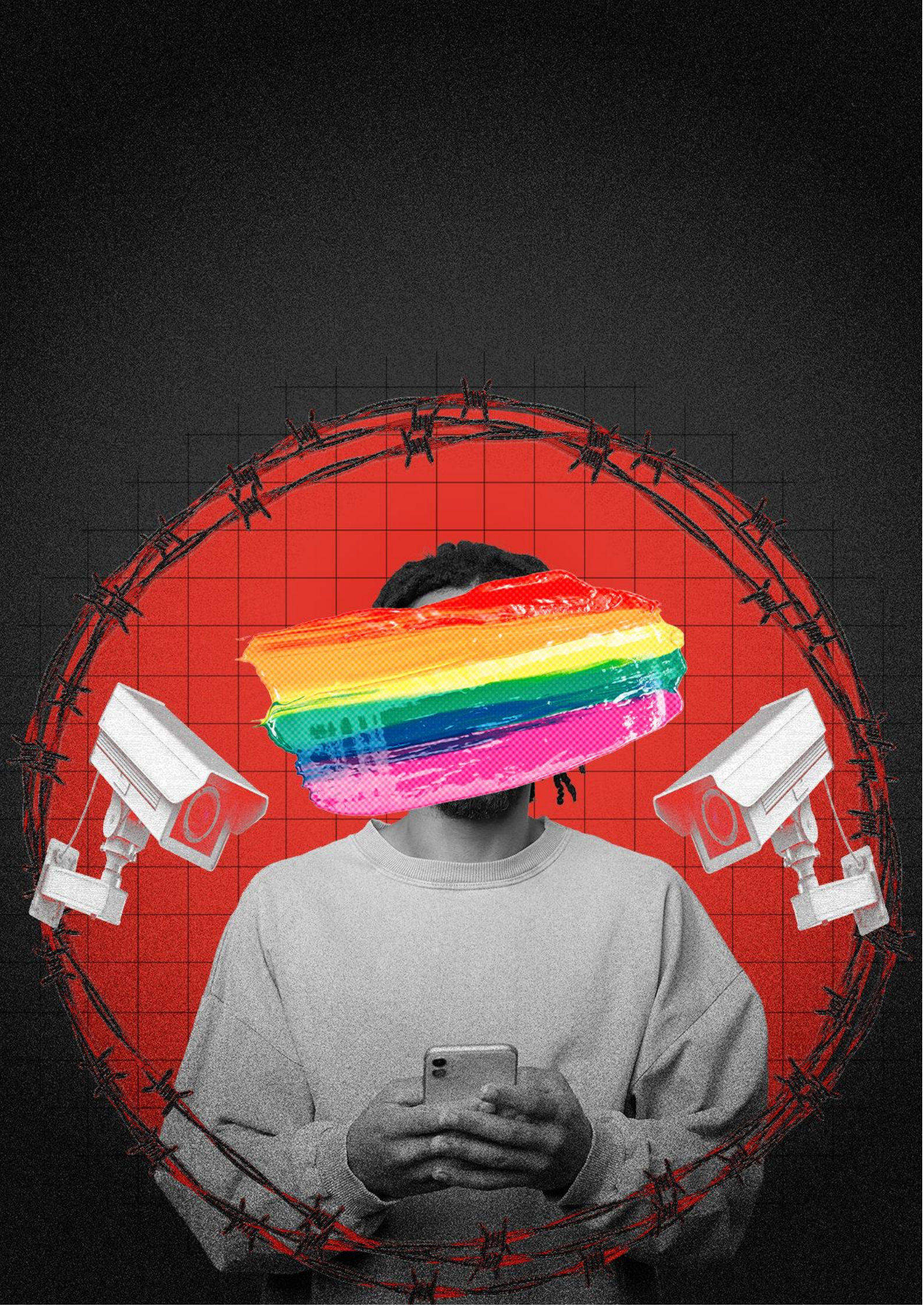
Similar to our interviews, the participants were selected based on experiences of either arrests, abuse, or violence based on their gender and sexual identities, as well as their use of technologies. ARTICLE 19 and local teams wanted to maintain a heavy focus on the highly marginalised members of the LGBTQI+ community where possible: refugees, sex workers, and trans people.

Table 3: Breakdown of 15 focus group discussions with 94 participants

Country	Location	Dates	No. of participants
Algeria	Oran	November 2021	5
	Algiers	November 2021	5
	Constantine	December 2021	5
	Skikda	December 2021	5
			Total: 20
Egypt	Cairo	December 2021	11
	Cairo	February 2022	9
			Total: 20
Lebanon	Beirut	June 2022	10
			Total: 10
Morocco	Rabat	December 2020	6
	Casablanca	June 2021	4
	Marrakech	May 2021	6
	Agadir	June 2021	6
			Total: 22
Sudan	Khartoum	August 2022	6
		August 2022	5
			Total: 11
Tunisia	Tunis	July 2022	5
		August 2022	6
			Total: 11

The outcomes of the focus groups included quotes, where provided, transcribed by in-country research teams, which the lead researcher of the project then analysed. As with the interviews, due to concerns for the safety of the participants and the complexity of the subject matter, the lead researcher manually and individually analysed the outcomes.

The data was used to inform a manual coding process which is reflected in the structure of the report.



Findings

State-linked arrests and abuses

Our statistics from just this round of research show the level of risk users faced only from arrests and police violence (on top of the other risks they faced):

Interviews:	**54 out of 93** (58%) interviewees reported they had experienced **arrests** of some sort.
Surveys:	**272 out of 641** (42%) people who reported state-facilitated abuses in our surveys by the police/state had experienced **arrests** and **159** (25%) had experienced **entrapment**.
Focus groups:	In **6 of the 8** countries (Algeria, Egypt, Lebanon, Morocco, Tunisia, and Sudan), in all the groups at least 3 persons had experienced **arrests**.

Over 20% of our respondents and participants had experienced arrest multiple times. These arrests included entrapment by police, on-street arrests, profiling leading to arrests, reports from other people to the police or security forces, or opportunistic arrests.

The number of arrests linked to protests and 'morality' policing in this research period stands out as a new finding. A high percentage had also experienced abuse by police. Numerous individuals reported 'honey traps', with individuals using fake accounts or motivations to meet them for financial or sexual extortion. Of these examples, a concerning number (around 53 different incidents reported to us) had involved police or other state actors and had used apps not only to lure individuals entrapment-style but also to extort money or sexual favours from people with threats of arrests.

Our research also shows an extraordinarily high incidence of police abuse and violence:

21 out of 93 *(23%) of our interviewees were trans (predominantly trans women) and* ***19*** *of them had experienced arrests.*

11 out of 93 *(12%) of our interviewees were sex workers and all had experienced arrests (a majority of them were also trans).*

In the cases of sex workers, the interviewees explained that their gender and sexual orientation meant that they were subjected to arrests and abuses whether or not they were working; this was especially the case if they were known as sex workers to area police.

9 *of our interviewees are refugees and* ***5*** *of them had experienced arrests.*

These numbers are only from our interviews and show how frequently those from highly marginalised backgrounds were subjected to arrests. A staggering volume of the interviewees recounted incidents of **rape by police as a weapon of torture**. Corruption, extortion, and other forms of abuse were prevalent, as seen below.

Our research shows a commonality across countries where non-state actors monitored the social media activities of LGBTQI+ people and then reported them to the police. In these cases where social media use led to arrests, it was either the police and the state conducting social media monitoring themselves or enlisting and encouraging non-state actors to conduct the monitoring and then to report individuals for queer activities to the police. Of concern in this new research is the vast use of social media monitoring (mostly by non-state actors) of queer people and the 'social surveillance' used to report individuals to the authorities. In effect, non-state actors are becoming proxy surveillers of LGBTQI+ people for the police.

Police abuse and violence

Police abuse and violence were a constant amongst all of our interviews. Throughout these interviews, focus groups, and surveys, police abuse was continually mentioned. The use and combination of police violence with privacy violations and general human rights

violations were accompanied by use of both new technology tools and traditional policing methods.

Interviews:	**60 out of 93** (65%) interviewees reported **serious police violence and abuse**, with some experiencing it multiple times.
Surveys:	**157 out of 641** (25%) people who reported state-facilitated abuses in our surveys by the police or the state reported experiencing **physical abuse and violent harassment**. This did not cover other types of abuse by the police/state. It did include rape, physical and verbal abuse, threats, extortion, robbery, harassment, forced anal tests, and two accounts of murder. Reports of the **use of rape** as a tool, or torture, physical and verbal violence, humiliation, and emotional torture were received in each country. Out of these, there were **7 direct cases of rape by state-affiliated persons**.
Focus groups:	In our focus group discussions that were held in **6 of the 8** research focus countries (Algeria, Egypt, Lebanon, Morocco, Sudan, and Tunisia), all mentioned **serious police violence and abuse**: all the Egyptian interviewees, **6 out of 10** in Algeria, and more than half of the participants in Lebanon, Morocco, Sudan, and Tunisia. **All sex worker, trans, and refugee participants had experienced police abuse.**

Tunisia

9 out of 10 *interviewees in Tunisia reported abuse and violence by police.*

Stories from Tunisian interviewees were harrowing and show vast human rights abuses of LGBTQI+ people by the police, which ranged from cases of rape, physical violence, and torture to false accusations and illegal use of solitary detention.

> *'They called me faggot, they hit me, they called me names, I had an eye infection because of the smells. They checked my photos when I left.'*

Trans interviewees and sex workers in Tunisia reported sexually violent abuses. For example, one trans interviewee recounted that two trans women were separated from the rest of the group and violently abused far more than the other cis detainees. The sexual and physical violence was without any motive other than abuse and extortion:

> *'Police [asked for] ID verification … we were begging them to let us leave, but he asked us to give him a blowjob under the bridge. … He slapped me and pulled [redacted name] by the hair, we started screaming.'*

Another Tunisian interviewee who was a non-binary sex worker experienced similar violent abuse and rape with impunity, as well as the use of false accusations to ensure they remained detained:

> *'I was raped the first time in jail by a guard. He wanted to have sex with me, but I refused, so he hit me, raped me, and said I was hitting on him, so they [gave] me four days in solitary [confinement].'*

For one of the Tunisian interviewees, an opportunistic arrest (see below) – which is when a charge like drugs or even just reporting a crime leads to an LGBTQI+-related charge – led to near-fatal violent abuses when the individual's identity was discovered:

> *'I went to file a complaint, but I was stopped instead. [The interviewee had a witness, but the police officer pushed him away and refused to acknowledge the witness to the crime our interviewee experienced.] I refused, so he hit me. I broke bones in my face, I had to have surgeries, I spent a lot of money, and I am still suffering. They made fun of me. I was humiliated.'*

In another opportunistic arrest, one Tunisian interviewee was accused of terroristic activities without charges. Their identity and the pretext of the criminal accusations were used for severe torture of the individual and the individual's family, supposedly to gather intelligence or a confession. The inclusion of the family has not been documented in our other cases. The intensity of the case demonstrates the impunity of police violence

especially if the queer detainee's charges are combined with higher 'national security' charges:

> *'I spent two days [in there] where I was tortured, and they hit me. They hit my family too. For a week they didn't let me sleep at all, they would harass me and not let me sleep for a week. They even sexually harassed me and raped me using objects while torturing me.'*

In the focus group discussions in Tunisia, the same issues came up, including how the push for access to personal electronic devices often led to police violence:

> *'I started seeing a police officer coming towards me, he hit me, took me to the police station and wanted to check my phone.'*

The experiences we documented in Tunisia followed the same patterns and types of abuse we saw in the other seven countries of the reports.

Lebanon

***5 out of 12** interviewees in Lebanon reported abuse and violence by police.*

All five interviewees were either trans, sex workers, or refugees/migrants, and in two cases they were migrant trans women who were also sex working at the time of arrest.

A trans sex worker interviewee recounted the violent treatment she was subjected to in 2021 when being arrested at her home, as well as during her time in detention, especially during the police's efforts to access her devices. She also recounted the torture of her partner, a Syrian refugee registered in Lebanon with the United Nations High Commissioner for Refugees (UNHCR) who was arrested with her. In this case, our interviewee highlighted that the police were in fact hired by a disgruntled former client she had met on a queer dating app. The police officer was on video calls with the client as they arrested and took our interviewee into the station in Beirut's Chevrolet area. This case alone demonstrates the layers of abuse, corruption, and illegal activity of state actors here, which was prevalent and experienced by the interviewees. Here are some of the extracts:

> *'All night, he was coming in every two hours, kicking me and asking me: "Where is the memory card?" I told him: "It's not with me." He said: "Why are you lying and denying what you are doing? You took it." He said: "I will cut you." … They brutally beat [my boyfriend] up because he was Syrian.*
>
> *They insulted us a lot. They beat us a lot. They threw accusations at us that we have nothing to do with. They forced us to say things we didn't want to say after the severe beating. My body couldn't take it anymore. My body is exhausted.'*

Another interviewee in Lebanon, who was also a trans woman, explained the intensity of the abuse from the police in the Hobeich Police Station – one of the most mentioned for police abuse – against a group of trans women who were arrested in 2020 based on their appearance and later accused of drug-related crimes in opportunistic arrests (see below):

> *'They were severely beaten. They hit them with a green belt and with sticks. They put them in a solitary prison cell under the pretext of not engaging with anyone. They called their parents. … They searched their phones and in all the content. … They insulted them, they spoke to them in the masculine form, and they also cut their hair. [Name redacted] had long hair, but when she got out, she was bald.'*

Morocco

***9 out of 10** interviewees in Morocco reported abuse and violence by police.*

The abuse and violence in Morocco showed similar patterns, and trans sex workers, again, faced the most abuse. One interviewee, a trans sex worker, outlined the abuse she has constantly been subjected to and how often she has been arrested, regardless of whether she was working or not, based on her gender presentation. The regularity was to the point that she only recounted the last arrest she had experienced, which had been 48 hours prior to our interview with her in 2021:

> *'My body hurts because of the 48 hours I spent at the police station.*

I met a person on Grindr and they interrogated us on the street in the touristic zone of Agadir on the way to the house. After an argument, they let him go and they took me to the police station to spend 48 hours.

I was there many times for 48 hours and once for 6 months and another time for 2 years. The details are almost the same [and] for the same reason. [Whether] I am with a client or walking alone, because of my feminine looks and the way I dress and walk, the police will arrest me. They are my nightmare. … As you see, I am a nonconformist looking person. I am a magnet to the police.

Each time it's an arrest, humiliation, and threats. I've been raped many times by police.

Because I am also a street sex worker, when I do not have clients available, I do the street.'

Another trans sex worker in Morocco explained profiling and targeting in her arrest in 2021 when corrupt police had only let her and her client go after the client bribed and paid them off – but not before they had subjected her to threats and verbal abuse. Importantly, the sex worker explained that she had had many security trainings in Rabat that helped her navigate this situation:

'I was once with a client. We were in the car. He went to buy something; I was waiting for him to get back from the shop. [The police] noticed me. Once he got back, they stopped us to ask about our IDs and ask embarrassing questions. They treated me so badly. They made me hate myself and my sex work.

They were homophobic and very intense. I was aware of the situation because of all the training I attended in Rabat. I tried to be smart. … I am aware of their tricks.

A lot of insults and humiliation. When they knew they were not going to arrest me, they asked for money. Then they tried to have sex with me. [They tried to] put me in a situation where they can either arrest me or at least have sex with me. They said we are doing this for you to become a man.'

Research in Morocco conducted by Akaliyat in 2020 included 400 LGBTQI+ people in Marrakech, Rabat, Agadir, and Tangier and showed the same patterns as identified in this research. It documented that those with nonconforming gender expressions were subjected to especially frequent arrest and physical searches without lawful reason. It also noted that 34% of those surveyed were 'subjected to harassment by the authorities, including insults, emotional blackmail, hate speech and intimidation during the investigation'. A third of the interviewed queer people reported that they had been subjected to physical violence and torture by a police officer.[1]

In their report, our Moroccan country experts also noted that it is overwhelmingly the community's sex workers who are subjected to these searches and extensive types of abuse and violence by the police:

> *'A sex worker in the streets of Agadir tells us that police routinely ask them for bribes or sexual services (usually fellatio) to avoid arrests for homosexuality (Article 489) or prostitution as a form of sex out of marriage (Article 490 of the Moroccan penal code).'*[2]

Algeria, Jordan, and Sudan

We see very similar cases in Algeria and Jordan.

---

6 out of 10 *interviewees in Algeria and Jordan reported abuse and violence by police.*

Often the violence was used to gain confessions, access devices, and gather further intelligence about the community, and of course for physical and financial extortion.

---

8 out of 10 *of our pre-war interviewees in Sudan reported abuse and violence by police in similar patterns.*

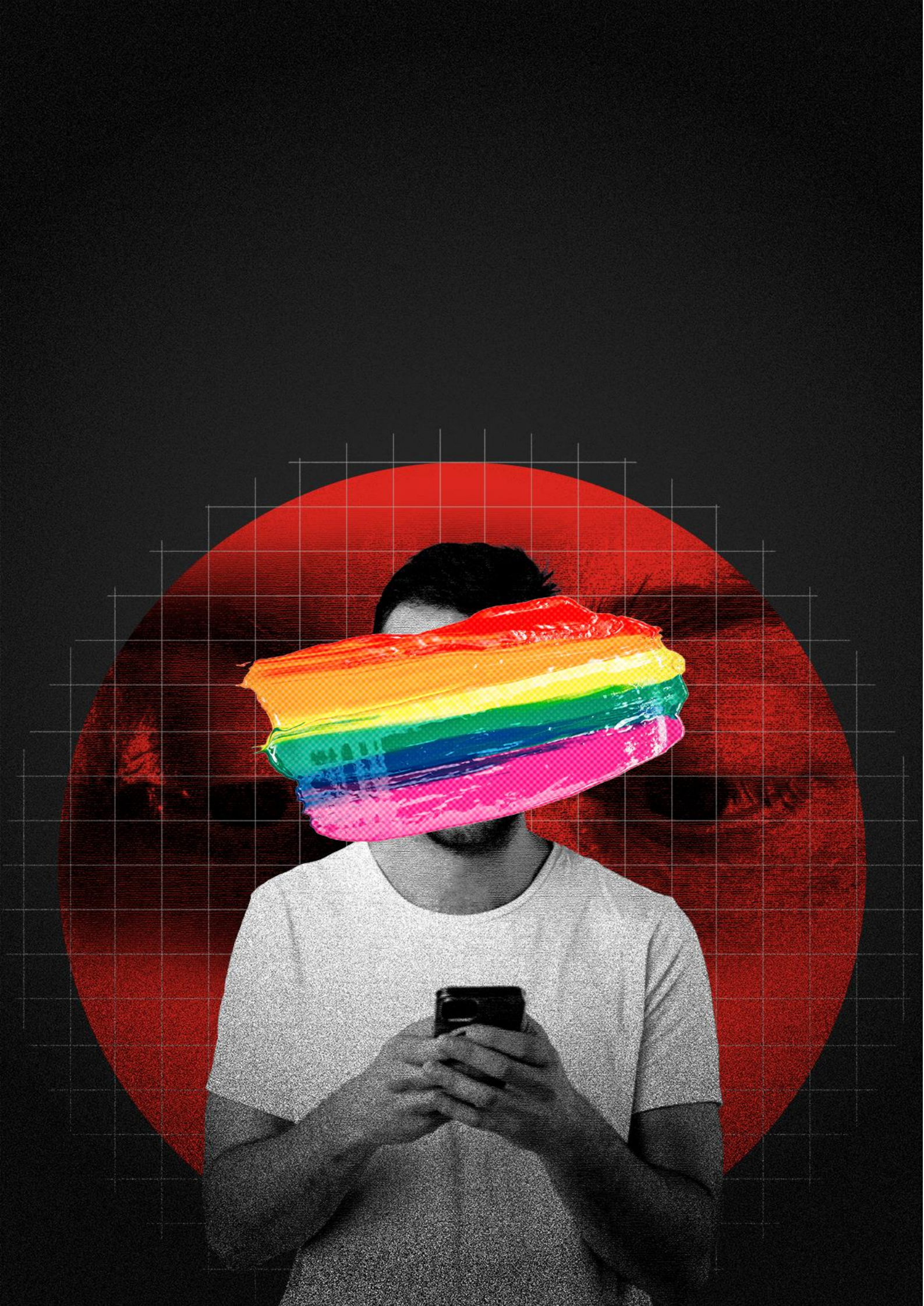
One of the gender-queer interviewees explained how they were subjected to intense levels of racism in their two arrest experiences. They were hit with 'whips' on one occasion in order to gain access to their device, which they had savvily hidden before being taken to the police van:

> *'In both cases, there was a flood of verbal insults that did not stop at all. Levels of racism to the extent of moral stigma and severe beating.*
>
> *The second time I was hit by whips, for my phone.*
>
> *I was beaten brutally and individually.*
>
> *We were subjected to the cruellest kinds of obscenity, insult, slander, and very incendiary words.'*

Egypt

***11 out of 11** interviewees in Egypt reported abuse and violence by police – the highest number amongst our interviews.*

The interviewees recounted severe, hours-long sessions where many experienced being beaten, raped, humiliated, and sent to solitary confinement. We also heard about cases of financial and sexual extortion as well as methods used to access devices.



Types of arrest methods

The following section goes into more detail about different types of arrests. It is notable that individuals were almost always faced with device searches in all types of arrests, so we have discussed this separately below.

Entrapment: police and fake profiles

Entrapment is one of the most orchestrated ways that LGBTQI+ people are arrested and targeted, by definition. In this context, entrapment is a term often used to describe a specific strategy of using fake profiles on social media or dating apps to fake romantic or sexual interest in individuals. Sexually explicit or otherwise queer-leaning conversations are thus elicited and, when printed, will provide all the evidence needed for the charge. Those involved in this strategy often then pick a meeting location where the individual is met by police or state-affiliated agents and arrested. In some instances, a secret informant is 'commissioned' to assemble digital evidence or act as 'bait'. This tactic is observed most heavily in Egypt. However, there have been more instances of copycat behaviour revealed through previous research in the region.

In our investigation, **10 out of the 54 interviewees who reported being arrested had experienced entrapment** (out of a total of 93 interviewees), specifically in Algeria, Egypt, Iran, Jordan, Morocco, and Sudan. In our focus groups in Algeria, Egypt, Morocco, Tunisia, Lebanon, and Sudan, **7 instances of entrapment** were mentioned.

In our surveys, **159 out of 641 (25%) people reported experiences of police/state entrapments**. The largest number was **102 entrapments in Egypt**, with the second largest being **25 entrapments in Tunisia**. In Lebanon, our surveys show findings of entrapment cases that were not previously fully documented.

Interviews:	**10 out of 54** (19%) who had experienced arrests (out of 93 interviews in total) reported **entrapment.**
Surveys:	**159 out of 641** (25%) people who reported state-facilitated abuses by the police/state had experienced **police/state entrapments**.
Focus groups:	In Algeria, Egypt, Morocco, Tunisia, Lebanon, and Sudan, **7 instances of entrapment** were mentioned.

*The most mentioned apps used for entrapment were **Grindr**, **Tinder**, **Hornet**, **Sugar**, **WhosHere**,[3] **Snapchat**, **Facebook**, **WhatsApp**, and **Instagram**.*

Whether police were using entrapment through informants, or doing it themselves and altering documentation, is an open question. When an informant is used, police can sidestep warrant requirements. Strong patterns present across these cases lead to speculation about how police officers in countries such as Egypt are trained to conduct these arrests. As our country-expert team in Egypt points out:

> *The police always claim that the person who helped them identify the accused must remain a secret informant and they must keep their identity hidden for their safety; as such, that informant remains anonymous throughout the trial.*[4]

In Egypt, our local partner and expert team outlined these methods of entrapment:

> *This [arrest] method is considered to be the most common one. … [After the arrest at the meeting spot] the police start searching the detainee's phone and printing out screenshots of the conversations they had with the individual on the dating app to present as 'sole' evidence of the crime the individual allegedly committed.*
>
> *The police also tend to fabricate their investigation report, as they claim they found information that 'proves' the accused committed the crime. They always include the accused's personal information as well as screenshots of the conversations they found on the person's dating app, the person's own profile on the app, and any*

> *personal or nude pictures and videos they found on the phone or received via the informant to add as evidence and present it to the public prosecutor.*[5]

In Egypt, many of the cases reported had the same pattern of police using fake accounts to entrap individuals. This excerpt is from a court file from the prosecution's case against an LGBTQI+ detainee from 2020:

> *Once we have received the tips and identified the targeted person and planned a date with him, we moved with our secret informant and a secret police taskforce to the place agreed on. Once we arrived there the informant conducted phone calls with the targeted person to make him come to the meeting spot and we saw the targeted person come in and we identified him through the pictures he sent to our informant. We sent out our informant to conduct a chitchat with him and the targeted person offered to have sexual relations with our informant and to take him back to his place to conduct these acts. Then we received the secret signal from our informant and we moved in and told the targeted person that he's being arrested for violation of the Cybercrime Law 175/2018 and Combatting Prostitution Law 10/1961.*[6]

In many cases, a lot of violence was also reported:

> *'A policeman trapped me through [Facebook] Messenger in 2018. I was arrested for 10 days, and I was humiliated. I broke my teeth also.'*

The main applications mentioned in Egypt for entrapment were varied: **Grindr**, **Tinder**, **WhosHere**,[7] **Facebook**, and **Instagram**. In our focus groups, **Tinder** and **Grindr** were also the most mentioned for entrapment. In our interviews, the most mentioned apps for entrapment were **Grindr** and **WhatsApp**. Often, individuals had been identified through social media or dating apps and then their conversations continued through chat-based platforms such as WhatsApp, Telegram, Facebook Messenger, or Signal.[8] In the case of Facebook Messenger, individuals could be identified (on Facebook) and could also continue the conversation on the chat-based platform (Messenger) in one place. This was the same for all the countries. The conversation from the platforms would then be used for evidence in court after the arrest and confiscation of devices.

Lebanon had **15 reports of entrapment** in the surveys, **5** of which were from Syrian refugees in Lebanon who described police and army entrapment in Syria. One respondent explained:

> *'In Syria [Homs], many security officers would create accounts on Hornet, and they'd text LGBTQI+ members in order to entrap them and take their phones so that they could arrest all the LGBTQI+ members they know.'*

The respondents also pointed to entrapment in Lebanon, where our previous research had not shown a specific trend of entrapment. For example, one survey respondent mentioned an entrapment arrest with trumped-up charges:

> *'I went to Dawra [for a date], and it turned out to be an intelligence officer. They beat me up, cursed me, and they arrested me for several cases like homosexuality and drugs. I spent three months at prison because I didn't have a lawyer.'*

Another individual reported entrapment by Hezbollah:

> *'I met someone from Hezbollah who pretended to be homosexual, and when I went to see him, I found that he set a trap for me. This happened in [redacted] 2021 in Dahye. I was arrested for two days where I suffered physical and verbal abuse and humiliation.'*

In Iran, we held no focus groups for safety reasons, but one interviewee explained that some cities in Iran are known for entrapment activities:

> *'Mashhad is a very security-concerned city. For example, you can say that out of every three people on Hornet, one of them is from the intelligence forces or police.'*

This person had experienced attempted entrapments at least twice in Mashhad and Tehran.

In our surveys in Iran, **9 people had experienced entrapment**. One respondent described unknowingly communicating with the Iranian Cyber Police (FATA) and being trapped:

> *'I once sent a message on Facebook to one of the FATA officers [who had a] fake account. He asked for my mobile number for a face-to-face meeting. Our address was registered with the same number. He came and arrested me, took my phone, laptop, and tablet to check. Some were just pictures. … The Revolutionary Court gave [just] a fine because it was my first record.'*

In Jordan we saw similar numbers from our participants, with **1 interviewee** and **3 out of 10 survey respondents reporting entrapment**. One of the interviewees, who was also a queer activist working on many abuse cases against the community, stated:

> *'Online entrapment cases were a trend for a while. At one point I was hearing of 13 different cases of this sort: entrapment then detention of people from the community. It's just authority figures making poor use of their power.'*

A queer sex worker in Jordan outlined the abuse from the police and their entrapment:

> *'Three years ago in January, in Amman, they lied and pretended to be customers, and they manipulated me by saying that they wanted to help me financially, without having sex. I figured out that they were policemen, and they arrested me, humiliated me, and exposed me to my family.'*

Though it seems this is not systemic in Jordan now, the abuse of power and violations without accountability hint at potential increases, especially as the environment in Jordan has continued to become more policed and oppressive around LGBTQI+ rights.

In Algeria, **4 survey respondents, 1 person in our focus group, and 2 interviewees reported being entrapped by police**. One interviewee who was also a queer sex worker explained how police used an informant, and only arrested them after the informant had had sex with the individual and left:

> *'I met a client on Grindr. I joined him in the hotel room. As soon as he left (5 minutes later), the police came to the room and took me to the police station.'*

Police-created honey traps: police and fake profiles

Arrests and prosecutions were not the only threats faced from the state. New and concerning findings in this research point to police and security forces using entrapment as a honey trap method – in other words, not for arrest but rather for extortion of money or sex.

Interviews:	**8 cases** of **police-created honey traps** were reported in our 93 interviews.
Surveys:	It is not clear exactly how many of the 159 people who reported experiences of police/state entrapments were victims of police-created honey traps.

Here, police and/or state actors **used entrapment to threaten arrest or violence**, only to then sexually violate, rape, blackmail, and/or extort from individuals. This scenario has come up very often in this research. The distinction is important here as the purpose in these cases is not always arrests or prosecutions but rather an abuse of power and the real threat of arrest or violence (even outing) to gain financial or sexual control of individuals.

The police and/or state actors use dating apps or other communication apps to lure queer victims and threaten them with arrest, outing, or violence to get what they want. Combine rampant levels of impunity and lack of accountability for grave human rights violations against the LGBTQI+ community with anti-LGBTQI+ laws, and the result is an environment conducive to these methods, including use of new technologies, not only for arrests, but also for sexual and financial extortion.

After entrapping an individual, police use the threat of arrest and violence to extort from individuals things such as money or sexual favours. The state does not hold to account law enforcement officers who use the criminalised and unprotected status of LGBTQI+ people to partake in similar abuses.

On top of such corruption and abuses on the part of police and other security forces, our research also shows them actively partaking in honey trapping through fake apps and using gathered knowledge of individuals' identities to extort from them financial and sexual favours with threats of outing and/or arrest.

Several times, police officers had used online dating apps to blackmail and extort money from queer individuals. One notable case was when, during the summer of 2020, a group of police officers in the city of Sousse, Tunisia, used the dating app Tinder to catfish (setting up a fake profile to trick people) queer men and then harass or blackmail them. This case led to civil society organisations communicating with the Grindr team in order to add extra security measures in the app.[9]

A similar case is linked to the 2020 Sousse incident of police entrapment on dating apps, when police, seemingly acting as vigilantes, targeted LGBTQI+ people through queer dating apps for abuse and extortion. The community came to know of these attempts to abuse and extort from them, and mobilised against it. One of our survey respondents summarised the situation:

> *'In June 2020, in the city of Sousse, a group of police officers was on Grindr targeting LGBTQI+ people and some of their victims were my friends. These officers would pretend to be interested in meeting someone or pretend to be clients for sex workers. Upon meeting the victim, they would beat them up in a hidden spot and as a group. … This happened to about 7 people. Thankfully, no arrests ensued. However, the victims were still beaten up and humiliated by this group of police officers. They seemed to particularly target sex workers and trans women.'*

These police honey traps that were focused not on arrests but rather on the threat of arrest were trends that our work had not documented to such a degree previously. This was specifically the case in Algeria, Egypt, Morocco, Sudan, and Tunisia, where in such cases there was no arrest but only threats of arrest and the use of power for this extreme abuse. Police were using new technologies for **police-created honey traps** for their own gain. At least **8 interviewees** described such detailed cases, with inflicted harms ranging from years of financial extortion to sexual trafficking among officers, rape, and severe

physical violence. There is **little to no evidence of any accountability or actions taken against these officers**. Often, due to fear of the state and criminalising laws against the LGBTQI+ community, there are no reports to authorities: how can you report wrongdoing when those you are reporting to are the abusers?

In Tunisia, a respondent to our survey explained:

> *'It is a very recurrent thing. Gay policemen in Tunisia, who are a minority, connect with us and try to scam people for the sake of blackmailing them and asking for money. They spy on us and submit our ID documents to the ministry.'*

One Tunisian survey respondent wrote that the extortion extended to other security officers who arrested and held the individual in prison as they continued to violate and abuse them without any accountability:

> *'In 2019, I met someone via Grindr. We matched and he sent me photos and agreed to have sex. Then when we met, he turned out to be a police officer, and he threatened to arrest me if I didn't have sex with him. After we were finished, he didn't leave me alone. He sent me security officers, who beat me and framed me under the Law No. 230. They kept doing what they wanted to me all night long, and they kept me at the police station.'*

Another respondent to our survey in Tunisia was entrapped, arrested, abused, and humiliated but not prosecuted, seemingly an abuse of power under the guise of 'morality':

> *'In Tunis I talked to someone [on Grindr] and he sent me his pictures, and we had a video call. … He turned out to be a police officer. He took me to the police station, and I was physically abused. They threatened to tell my family about me, and they really frightened me. At that time, I didn't know any organisations or associations and I was all alone.'*

Our Tunisian country experts further explained these incidents:

> *In the past few years and due to the rise of dating applications, the number of assaults against LGBTQI+ individuals keeps growing. Most of these assaults are*

> *perpetuated by straight men or police officers, and the most affected populations are gay men and trans and gay sex workers.*

An Egyptian interviewee described a similar experience in 2021 after discovering that their date was a high-ranking police officer in Cairo:

> *'[He said he was] working as a police secretary and that he would hand me over if I did not comply with his threats, and when I did not comply with his requests, he called on two people [to come] out of the room, and the three of them forced me to get off and [then] forced me to get into a taxi, and they took me to the Maadi police station, where it turned out that he was really a police secretary in the station.'*

Another Egyptian participant, this time in our survey, reported the same experience:

> *'In April 2019, I dated someone on Grindr. He came to my house in Cairo. He entered the house with three other men who said they were the police. They searched the house and stole the belongings, threatening to expose my photos to my family and relatives, and they took my mother and siblings' phone numbers. I didn't take any measures.'*

In Sudan, similar accounts of intelligence officers using apps to meet, then using threats of outings and arrest to extort, were reported in **2 of our interviews**. There were **3 cases of entrapment** reported in our surveys and **1 in our focus group** discussion, where a security officer honey-trapped the individual on the geolocation-based dating app Sugar.

The police-created honey traps show the level of impunity for violence against queer communities. It was thus unfortunately not surprising that some of the biggest issues on apps related to non-state-linked honey traps used to sexually violate, rape, blackmail, and/or extort from individuals.

Street arrests: profiling, protests, and street patrols

Physical surveillance of individuals, localities, and public spaces for 'criminal activity' is one of the oldest law enforcement investigative tools.[10] Here, 'street-level physical surveillance' is the act of police and enforcement authorities profiling individuals based on

their physical appearance and perceived gender and sexual identity, which leads to stop-and-search methods or arrest. We also document the use of 'morality' policing. As with previous reports, this tactic has continued to be one of the main methods used to arrest or identify LGBTQI+ people in each of the eight countries discussed in this report. The prevailing classist, homophobic, and transphobic attitudes across all levels of law enforcement form the foundation of this mode of targeting queer people.

The surveillance element is an important one: law enforcement methodology goes beyond merely stopping people who are judged to be suspicious due to their apparently queer bodies. In many cases, police are actively looking for queer people on patrols or active searches, and then using physical profiling to single out individuals. Known hangouts or places of congregation are the places most surveilled.

In our research we saw the prevalence of this method of arrest.

Interviews:	**28 out of 93** (30%) interviewees reported **on-street arrests**. There were 2 reports in Algeria, 2 in Egypt, 2 in Iran, 2 in Jordan, 5 in Lebanon, 4 in Morocco, 7 in Sudan**,** and 4 in Tunisia,.
Surveys:	Since we asked our respondents to focus on technology-related arrests, an exact number has not been gathered specifically on the issue of on-street arrests in our survey. That said, there were more than **60 mentions of arrests** linked to street-level physical surveillance out of the **272 reported arrests (out of 641 people** who reported state-facilitated abuses in our surveys by the police/state).

On-street arrests in Egypt, especially through surveillance patrols on the streets, are well documented, and are often made through informants. Our country experts in Egypt pointed this out:

> *This is a common method where police officers rely on secret informants to gather information on the known meeting spots for the LGBTQI+ community. They then*

use this information to determine where to set up checkpoints to target the LGBTQI+ community in places like Ramsis Sq. and Gamat El-Dowl St.[11]

An important and interesting case is one from Egypt where an individual, who was prepared and very safety-savvy in dealing with police street stops and patrolling, was still arrested due to a surprise notification on their phone. They were walking through a protest area that they were not involved in and were stopped by the police based on their appearance. But there was nothing on their device to endanger them (as they had pre-planned for such a device check) until a notification came through on WhatsApp that was not muted. He was arrested, detained, and subjected to abuse, attempted rape, and violence:

'This incident happened to me on an application in November 2022, where there were calls to demonstrate against the ruling Egyptian regime in Tahrir Square on 11/11.

I left my house heading to work and, as I expected, I was stopped at the entrance to Tahrir Square and forced to open and search my phone, but they did not find anything on it. When the police secretary wanted to return my phone and ask me to leave, something happened … one of the people I knew through the Grindr application, and we exchanged WhatsApp numbers, sent me a message containing sexual suggestions, and then pictures of his penis, and the police secretary opened it immediately, and he insulted me and hit me on the face, and asked me to ride in the [car], and I stayed there from morning until in the afternoon.

We were interrogated, and at night the officer stood at the detention door and told the prisoners:

"By the way, this boy is like me. You can entertain him until the day when he doesn't come out." After that, I was subjected to harassment and attempted rape.

The next day, I was interrogated again in the police station, and I insisted …that I didn't know the sender of the message, especially since his number is not registered on my phone.'

This individual was luckily released as they managed to deny knowing the sender and there remained insufficient evidence on the device to prosecute them.

This tactic was used not only on the streets, but in any public space queer people congregated or frequented. Those with multiply marginalised identities were the most at risk from the tactic because it relies so heavily on profiling, and wielding of power over those with the least access to recourse from any systems of justice.

In Morocco, a gender nonconforming interviewee told us about an incident where 24 people in a garden gathering had been arrested in 2021. This individual had experienced many incidents of arrests on the street or in public due to their gender presentation. During this incident in the garden the interviewee mentioned that only the gender nonconforming people were taken, and the pretext was a murder that the police had linked and used as a reason to gather queer people. They were subjected to torture, violence, and humiliation with no accountability from the police or the system responsible. Police lied about the conditions of arrest in order to arrest them (see below):

> *'One day I went to a public garden where the community hung out because we used to consider it a safe space. I was hanging out, then without any notice police entered the garden and took all the gender nonconforming people to the police station.*
>
> *They arrested us all … they asked for IDs. They arrested 24 LGBTQI+ people.*
>
> *A European gay man was found dead. They took all of them for 48 hours. They wrote in the report that they caught me in action having sex and threatening the morals of society, which was not the case. I refused to sign the report.*
>
> *They beat me and I was obliged to sign.*
>
> *I got arrested for six months.*
>
> *They took my pictures with a banner in which was written "homosexual". They did not allow us to go to the toilet. They were misgendering us. They insulted us. … It was very humiliating. I got sick after that.'*

In Morocco, another interviewee who was a trans sex worker explained how she was often subjected to abuse and arrest whether or not she was working. She recounted cases of arrest, highlighting only the ones from the recent past due to their frequency. Nevertheless, she explained that in each case the details were often identical. With sex workers, regardless of catching them with other queer people, the police would often let the clients go and arrest, abuse, rape, and prosecute only the sex workers. This held true especially for trans women.

In many cases, there was evidence that police were actively patrolling the streets for queer people to arrest through their physical surveillance of the streets. This was often – if not always – followed by device inspections for further 'incriminating evidence' for their arrest and prosecution. This is further examined below.

Our Moroccan country experts noted that it is overwhelmingly sex workers of the community who are subjected to these searches and extensive types of abuse and violence:

> *'In [February 2020], during the same periodical meeting of Moroccan queer activists in Marrakech to launch the queer movement coalition in Morocco, the activists noted that a routine part of the life of many LGBTQA+ [lesbian, gay, bisexual, transgender, queer/questioning, asexual] people especially sex workers is to get [searched] because of moral judgments and profiling by police.*
>
> *As per the experience of many queer sex workers recounted to us from on the ground, police assume that any person with gender nonconforming expressions is a homosexual. This assumption leads to fast searches and investigations with the person and often lands the person in jail. [Here the team also explain that sex workers are subjected to rape and sexual exploitation by the police in exchange for not being arrested.]*
>
> *Sex workers practising in the touristic zones are the most vulnerable to the police. This is especially by the Tourism Police who are operating specifically in touristic cities such as Agadir, Marrakech, Casablanca, and Tangier. [They] are aware of the*

existence of dating applications such as Grindr, Hornet, and PlanetRomeo, so they search phones for them specifically.'[12]

***1 out of 10** (10%) of our Algerian interviewees reported an on-street arrest, and once again it was the experience of a trans sex worker targeted for her gender presentation.*

***4 of out 10** (40%) interviewees in Tunisia had been arrested on the streets, all of them multiple times.*

Again, trans people or those who were coded as gender nonconforming were at most risk. One Tunisian interviewee explained:

'They just asked if I was a boy or a girl, and they slapped me at the entrance to the station. … On the way to the police station, in the police car, I found a trans sex worker also arrested … they assumed I was with her, and they hit me. Then they looked at me, and asked me if I agree with her looks; at first I didn't say anything, then I said everyone has the right to do what they want.'

The same occurred in Lebanon, which had the highest number of interviewees who had experienced this method.

***4 out of 5** (80%) interviewees in Lebanon who had experienced on-street arrests (from a total of 12 interviewees) had experienced searches or arrests at checkpoints.*

One survey respondent from Lebanon reported that they were currently waiting for their proceedings from an arrest from this tactic:

'In 2019, I stopped at the police checkpoint at the airport, and they opened my phone and saw the chats on my phone on Facebook and Grindr, so they arrested me for 2 days. I'm still waiting for the procedures.'

Our country experts in Lebanon have explained how this is linked to perceived gender identity and non-heteronormative 'behaviours':

> *The case law and published reports have revealed that in a big number of cases, individuals prosecuted on the basis of Article 534 of the [Penal Code] are identified and stopped by the judicial police based on their appearance and their 'behaviour' and 'speech'.*[13]

In the 'Hammam al-Agha' case, which led to the arrest and prosecution of 28 individuals, the investigation was initiated by the General Directorate of General Security, whose investigator, in the course of interviewing a Syrian refugee for lost identification documents, found his behaviour and discourse to be 'uneven'. The officers decided therefore to conduct a search of his mobile phone, which contained 'sexual videos of males amongst themselves, as well as exchanges of a sexual nature between [the foreigner] and others, about massages and sexual acts'. After being informed about the case, the Public Prosecutor of the Appeals Court in Beirut decided to arrest the refugee and refer the case to the Morals Protection Bureau of the Internal Security Forces for further investigation.[14]

Our country experts went on to report that the most affected people are often trans women who were simply being trans and became targets of on-street arrests:

> *[This] initiated the prosecution of several trans women where the Public Prosecutor and/or police officers detained trans women based on suspicion of 'prostitution' without any other evidence than their appearance.*[15]

In Iran, interviewees discussed several incidents where they had been apprehended on the street while having an intimate moment with another person. The intimate moments ranged from two gay men holding hands on the street in Isfahan to two gay men kissing in a car in Tehran to two gay men having oral sex in a car in Tehran. The morality police were in charge of the case in Isfahan – the two men were taken to the police station and released after signing a statement.

Cruising areas and queer hotspots like Daneshjoo Park and College Bridge in Tehran are regularly patrolled by police officers. The areas have been flagged as 'unsafe' and a 'hotspot for sodomites' by Islamic Revolutionary Guard Corps-aligned outlets.[16]

Similar issues and fears were expressed about the checkpoints in Sudan pre-war. It is assumed these have become much worse during this current war.

Checkpoints and the multiply marginalised

In Lebanon, police and army checkpoints are frequent occurrences in everyday life and can create points of contact between law enforcement and marginalised groups, including Palestinian and Syrian refugees and queer people. Checkpoints are doubly risky for queer refugees.[17] Trans people and sex workers are also highly vulnerable and targeted at checkpoints in Lebanon.

Our trans and refugee interviewees held more than one of these identities and were thus not surprisingly the most impacted here. This subjugation was further affected based on socio-economic status. One interviewee, who was a trans refugee, described this dehumanising experience at a checkpoint where after her detention she had needed to get support from the UNHCR offices:

> *'I was headed to the centre in a taxi and he stopped at the checkpoint. … He asked to give him my ID and I did. When he saw the ID, he told me that the ID is not mine. I told him yes, but I am a trans woman. … He asked me to step out of the car. … The officer kept me under the pretext that I had stolen the identity card.*
>
> *He started asking me: "Why are you [like] this? Why are you dressed up like this?" He was talking to me using the masculine form. His friends gathered around him and started bullying me. After that, he started searching my bag.*
>
> *They started asking me about my legal documents, and if I carried any. … I called the UN and told them that I was detained and I don't know for what accusation and that they were not letting me go.'*

Another interview from Lebanon further exemplified this compounded harm of multiply marginalised identities. This interviewee was a trans woman and a sex worker who was living a heavily impoverished life. For her, her mere existence was a reason for arrest and harassment by police due to her gender and the power-wielding of these forces against her. Although she was a sex worker (which, in its criminalisation, is complex in Lebanon**,** and street-based sex work is illegal), she had never been arrested while working, but rather multiple times while she was living her life:

> *'But let me tell you that I was never detained with a client in a car. Or during my work hours. They arrested me while practising life normally. Like going to the pharmacy to get medicine for my mother.'*

Up until the date of the interview in early 2023, she had been arrested seven times. One arrest was pre-gender-affirming surgery, when her clothing and look were the sole reasons why she was picked up, abused, and violated:

> *'I was with my friend, and it was her birthday … I was like everyone else, dressed up for a party. But my clothes were modest. I mean I was wearing pants and a crop top. But back then, I hadn't made any changes to my body.*
>
> *And suddenly, they came and detained me. They hit me and took me to the Gemmayze area where I spent two days.*
>
> *They detained me, hit me, and were very violent with me. They were insulting me while I wasn't guilty and had done nothing wrong. [Later] a plain clothed officer tried to rape [me] in the toilets in the precinct.'*

In Iran, the morality police and state-backed Basij (Islamic Revolutionary Guard Corps-controlled militia) regularly set up checkpoints through major cities – especially in Tehran and Shiraz – inspecting pedestrians and passing vehicles to enforce hijab rules and the ban on alcoholic drinks and drugs.[18] This has led to device searches, confiscations, and arrests.[19]

Of course, every case and interviewee has been subjected to device searches (see below).

Political and protest-related arrests

***12 out of 93** (13%) interviewees reported political or protest-related arrests.*

There has been a recent uptick in arrests of queer people linked to political activities – such as at protests – while also using 'morality' policing policies. In other words, gender and sexuality profiling happened during these movements and protests, and other policies were used as a pretext to also police their identity. For example, in Tunisia, **3 of the 4 individuals** who had experienced on-street arrests (from a total of 10 interviews) had been arrested multiple times and reported that they were at recent protests and uprisings at the time.

In 2021, protests erupted in Tunisia against the socio-economic and political situation. These protests were met with severe brutality by the Tunisian police, including the large-scale targeting, harassment, and arrest of LGBTQI+ people involved in the protests – much of which included digital surveillance and monitoring. These arrests included the highly controversial arrest of Rania Amdouni, who is a well-known queer activist. Three of our interviewees were later arrested based on their connection, or perceived connection, to Rania, her queerness, and political activity. One of our interviewees said that they were accused of being part of the protests due to one of the tagged photos of Rania and accused of obstruction even though they were not involved in the protests:

> *'I was involved in this case [the police] saying I was blocking a road, and then, when we went to see what [was] the problem, turned out they checked Rania Amdouni's Facebook profile, they found a post she posted and tagged our names in it, every single person that was tagged in that post was part of this case.'*

This included a queer friend who was also summoned to court even though they were not in Tunisia at the time of the protest.

In Sudan, **7 out of 10** pre-war interviewees had experienced on-street arrests and/or searches (multiple times) and 5 of these were during protests. These were predominantly during the 2019 protests and revolution. One interviewee described the Sudanese context:

> *'The arrest is usually political, but then [also] allegations such as you are "twisted", for example, you are a girl or for your orientation. … I was arrested in a demonstration in February 2019 in Khartoum. I was arrested along with a lot of people from the demonstration, and they took us to the office of the security services. Those who arrested us were members of the security services wearing civilian clothes. There was beating and verbal and physical abuse and threats of rape and racism and all kinds of violations.'*

In Iran, the Islamic Republic's security apparatus systematically weaponises the private lives of activists and political figures to pressure them. Iran's uprisings, such as the massive protests in 2009, the November 2019 protests, and the mass Aban protests in 2022, as well as the 2022–2023 Woman Life Freedom protests, have resulted in repression, deaths, and thousands arrested. The queer community's prominent presence was seen in the 2022–2023 Woman Life Freedom uprising, which was in part against the abuses of the Iranian morality police. During these protests, many queer people were arrested and risked having their identities outed. However, even prior to these protests, queer people continued to be harassed and arrested especially via on-street arrests by the morality police. In Iran, **4 out of 14 interviewees had experienced arrests and/or device searches due to the morality police**'s perceptions of the breach of Iran's mandatory hijab laws, as well as for other political activity.

In Jordan, protests have continued throughout the years for varying political and economic issues. In 2021, solidarity protests with Palestinians led to monitoring and potential arrest of Jordanians. One of our interviewees noted:

> *'They were monitoring us on Facebook.'*

Opportunistic prosecutions

9 out of 93 *interviewees (10%) reported opportunistic prosecutions and arrests, specifically.*

As identified in previous reports, a very common path to prosecution for LGBTQI+ individuals is through unrelated contact with law enforcement authorities, such as reporting a crime or being involved in another case under investigation. In this research, we saw examples in Egypt, Iran, Lebanon, Jordan, and Tunisia, especially in the interviews and focus group discussions.

When investigators, prosecutors, or police gain access to an individual's device and the digital evidence on it, they are able to start creating a case based on the individual's sexual or gender identity.

Any contact with the police or police station in these scenarios leads to arrest, often due to profiling and device searches. In some cases, individuals are brought to the police station in connection with another case and when their identity is discovered they are charged under the myriad anti-queer laws. On other occasions, they are arrested using anti-queer laws or policing for other purposes. The latter was documented in Iran and is a known phenomenon, as one interviewee reported:

> *'Arresting people just for being queer is a possibility, but because this has human rights costs, they used it less. Mostly, they use this issue as a lever to put pressure on people [politically], like what happened to my friend.'*

This individual clarified:

> *'But in general, people are likely to be arrested for being queer, especially in small towns.'*

In our Tunisian focus group discussion, one participant observed how these types of opportunistic prosecutions develop unrelated to the initial point of inquiry:

> *'My friend was called during a murder investigation because the person who died talked to him for months. They arrested him based on Article 230 [of the Penal Code 1913] because they found out that he is gay.'*

In another case, the interviewee was arrested in 2020 under the charge of robbery. They were acquitted of this charge but still charged under Article 230 of the Penal Code 1913 due to the contents of their device:

> *'I got jailed for four months.'*

In numerous cases, in all the countries of our research, people reported going to the police to report lost phones, harassment, stalking, violence, theft, extortion, rape, and many other abuses to which the LGBTQI+ community is especially vulnerable. Yet in these instances, when their identity was discovered, the case was not processed or, even worse, they were charged instead under anti-LGBTQI+ laws. In any instance where the **device falls into the hands of authorities, the individuals are immediately under risk**.

For example, one of our Tunisian interviewees recounted a brutal turn of events when they went into the station to file a complaint after being robbed, but instead they were profiled and brutally and violently beaten:

> *'I went to file a complaint, but I was stopped instead. I went because I was robbed in the streets, in Korbes. I called the police using someone's phone, I had a witness who knows them and knows where they live and all. … When the police came, I told him this is the witness, he looked at him, then pushed him away and told me no, there is no witness at all. And he started insulting me. He told me it is ok and started making fun of me, saying it is nothing. … He wanted to get me in the police car, but I refused so he hit me. I broke bones in my face, I had to have surgeries, I spent a lot of money, and I am still suffering. They made fun of me, and I was humiliated.'*

This lack of protection and flagrant violation of rights is very common when LGBTQI+ people cannot trust state entities to report crimes, knowing they risk being arrested

themselves. Criminals often seem to know this to be the case and target LGBTQI+ people as a result, creating a layer of immunity for themselves.

One interviewee in Morocco, who was severely beaten, robbed, and raped by criminals, was dismissed after authorities saw the individual's device and identified their sexuality. They said the police had told them that:

> *'My case was not considered rape because [they accessed] my phone. They found photos, applications, and everything.'*

In Jordan, in a case where police were called to deal with an altercation, many trans people were arrested and violated further when police published their photos online:

> *'A group of LGBTQI+ folks, mostly trans, who were in a gathering in Jerash [governorate north of Amman]. They were in a private house and there was a disagreement that occurred in the place, and someone called the police … and the police came. Instead of resolving the issue, the police arrested them based on how they look. The police took pictures of the detainees and published them on news platforms.'*

In other cases, people have often been profiled based on their gender and sexuality, and a pretext of other 'crimes' has been used to access their devices and detain them for both the pretext crime and their sexuality. In Lebanon, at least **2 interviewees** pointed to drug-related opportunistic prosecutions in 2021. One of these cases involved a group of seven mainly trans women and was violent and deeply concerning, further demonstrating the violations of human rights and corruption within the policing system:

> *'My friends were changing their clothes and wearing make-up where they were. Suddenly, the white car passes me and parks in front of me blocking my way. They got out of the car and asked us to give them our IDs. They introduced themselves as detectives with the Ramlet el Bayda branch. … He told me that I have to be interrogated before the party to understand what my friends were doing.*
>
> *They took us to the Ramlet el Bayda police station … [they were in civilian clothes]. They took us to detention with [our] party clothes. They asked us if we used drugs,*

and I answered that we didn't. He said he would give us a blood test to be sure. … He told me: "So were you getting fucked? I want to test you."

He said: "Open your phone." I said: "I will not open the phone. There are private photos of me and my siblings. You can't open my phone."

Then they handcuffed us all. There were seven of us. They put us all in the lieutenant's office and made us sleep on the floor. … I wasn't used to such places, and I couldn't use the toilets there. So, they threw water on my back to make me pee. After they did the blood test, it showed I was clean and not on drugs.'

The police continued to abuse them as the arrest was not about the drugs – the drugs were a pretext for an identity-based arrest.

'They bullied me and humiliated me. They told me that I can leave but asked me to take off my bra and break my nails and not wear such clothes in my life. My friends had also done the blood tests, and some of them their results came in positive. Those were taken to the Hobeich centre and were tortured. They humiliated all of us a lot. … They beat them brutally. They were subject to excessive violence. And they stayed for 17 days at the Hobeich centre before they could leave.'

Often the aim of the authorities is to get the highest number of charges, and so combining homosexuality charges with other crimes is a very common and symptomatic element of opportunistic arrests. This was indeed the case with the following incident where police combined 'homosexuality' charges with prostitution and drugs, even when the victims were simply existing on the streets:

'They took them in for "homosexuality" and drugs. They didn't accuse me of "homosexuality" at the Ramlet el Bayda station. When they asked what happened to them, they told me they were detained for accusations of "homosexuality" and drugs. … At the Hobeich centre they assumed my friends were practising prostitution when they were only standing under the Cola bridge.'

In Iran, LGBTQI+ individuals are also caught in parallel cases related to drugs, the alcohol ban, or hijab rules. Iranian security forces also use queerness to pressure political activists

and coerce confessions. Usually, if the interrogations happen on the streets, they are initiated at police or Basij militia checkpoints or during random stop-and-search incidents on streets.[20] In some of the incidents mentioned by our interviewees, individuals were released through bribery, while in other cases the individuals were held in police custody for several days before being released on bail.

Reports and social patrolling

Another method that has led to arrests, harassment, and prosecution of queer people is official complaints lodged with the police, as outlined in our research. These reports may be from neighbours, from staff at businesses patronised by members of the LGBTQI+ community, from people patrolling an individual's social media, or from a variation of these methods. Motivations behind these reports vary immensely – from disgruntled ex-lovers and revenge to plain homophobia and the use of privilege and power to enlist the force of the law. In many such incidents, people were reported on based on 'suspicious' activities pertaining to an individual's appearance, for example looking 'effeminate' or generally gender nonconforming. Many of the cases reported to us were from parties or gatherings deemed queer where **large groups were arrested and searched**.

---

11 out of 93 *(12%) interviewees mentioned situations where reporting or informing had led to their arrest.*

This was the case in Algeria, Egypt, Iran, Jordan, Morocco, and Tunisia. Our interviewees in Lebanon and Sudan did not report this type of arrest. In the focus group discussions, there was less discussion of these strategies, but in Egypt, Lebanon, and Sudan they were still documented. A more extensive review of the thousands of survey responses needs to be done to confirm the exact numbers in the surveys.

Revenge reporting

Bad faith and revenge tactics have been common in these cases. Many individuals were reported on by people they knew who used their vulnerability and risk against them. In Tunisia, there was a case where queer friends befriended and tried to help two women

who did not have a place to stay. After the queer friends realised they could not house them due to safety concerns, the women reported them for being queer and got them arrested:

> *'They didn't have a place to stay, both these girls, and their father was very well known from Libya and they were looking for them. When we found out about this, we told them to find a new place because we were scared, and we were all in danger because of this, so one of those girls filed a complaint against us, saying that we have parties at home for gay men. That's how the police knew about us and came to our house. … They found in our house women's clothes and perruques [wigs] they used against us … they saw us, we look "gay", they found clothes, and based on all of that, they based their verdict on Article 230.'*

Often in these cases the complaint lodged is filled with falsities, but the law remains on the side of prosecuting queerness. At the moment of being in contact with law enforcement, individuals are profiled based on their gender and sexual orientation, and arrested with little to no evidence.

In another similar revenge reporting case in Egypt, a disgruntled, rejected suitor of a lesbian interviewee gained access to the individual's Facebook account, which she had logged into from her work computer. He used it, saw her messages with another woman, and used these messages to out her to her family:

> *'This happened in 2019 while I was on the Facebook application, where I used [Facebook] at work and communicated through it with the work team [at] the newspaper.*
>
> *One day, my boss asked me to marry and when I refused, he searched my Facebook account in my old posts until he reached my posts in which I expressed my relationship and my love for another girl.'*

These events led to her being locked out of her home and cut off from her family, and the end of her journalism career. He continued to harass her without her being able to block his numerous new accounts:

> *'I blocked his account on Facebook and Messenger, but to no avail, as he was adding me and sending messages on the Messenger application through a different account. … After that, I changed my phone number and deleted all my accounts from the social media accounts (Facebook, Messenger, Instagram, WhatsApp) and I left my journalism profession permanently.'*

In a common but heartbreaking turn of events, when our interviewee attempted to report this continued harassment to the police, she was herself summoned to the Prosecution Office with the blackmailing information used against her, not the perpetrator:

> *'I later tried to report him through the Internet Crimes Police, but the result was the opposite, as I was summoned to the Public Prosecution Office, and it turned out that when they summoned him for interrogation, he told them of my inclinations and showed them some screenshots of the conversations he was trying to blackmail me with. … I denied my knowledge of them.'*

Only the fact that she had closed her accounts helped her avoid sentencing:

> *'And what helped me in denying that [is that] I had closed the Facebook account and was released from the Public Prosecution on the guarantee of my place of residence.'*

This Egyptian case is one that combined reporting with opportunistic arrests, which is a very common overlap.

In Jordan, one interviewee reported a case involving this tactic that was about an event they were connected to – and one to which the state had been alerted. They were summoned for questioning, which was followed by intense interrogations about their connection to the queer community, their views on the community, and other intrusive topics:

> *'Last year – we're under martial law now – and I got called in last year by the governor's office and I was interrogated over the [redacted] in Amman. [Redacted] had organised a webinar for pride month on LGBTQI+ rights in the Middle East which was cancelled by the governor. The governor had found out about it, and it*

> *was a big deal online and they thought I was one of the organisers and I wasn't, so it was like a three-hour interrogation of them accusing me of being a part of it and me saying "No".'*

This individual was well connected and versed in interrogation tactics so they were not intimidated. They also denied their involvement with the event. Both meant that they were able to be released and left without charges.

Reports by foreign nationals on local LGBTQI+ people (and the reverse)

Interviewees outline very specific and clarifying incidents of how this kind of reporting happens and how technology becomes part of the strategy.

One of the clearer themes that shows how arrests and abuses of the community have been heavily linked with power is how **foreign nationals – especially from Europe – have been spared any arrests or prosecution**. And in more heinous cases, they have used this knowledge of their race and nationality privilege to inflict harm on local and more marginalised queer people. For example, in Morocco, a gender nonconforming queer sex worker explained how they had been arrested numerous times. One of the incidents they wanted to highlight was with a gay white French man. The interviewee had decided they didn't want to sleep with this individual. This individual reported our interviewee to the police as gay and a sex worker, and accused them of stealing his laptop. This act of power and aggression landed our interviewee in jail for two years:

> *'It was a French old man I did not want to have sex with who declared me as gay and that I stole his laptop, which I did not. I found myself spending two years at jail. I still can't process this one. I felt alone. … He is also gay, but they did not arrest him. They do not treat Europeans the same way as us. We are the weakest link here.'*

This same individual was also reported by a Saudi person, and, again, only they were arrested because the Saudi individual was rich and a foreign passport holder. In these reports a person's multiply marginalised background is used against them heavily.

In Egypt, there was a similar case where a queer party organised by someone on a dating app was reported, but only Egyptian passport holders were arrested:

> *'When one of us showed a foreign passport, they left him and asked the person next to him. They remained in this state until all … persons holding Egyptian passports were taken. … We were taken to the October Police Station, and there we received a torrent of insults, physical assault, and harassment.'*

In a reverse of the above two situations, another Moroccan interviewee who was a refugee from abroad outlined how the police not only responded to the report of neighbours without any question, but also proceeded to confiscate the interviewee's papers and residency permits:

> *'[Report from a neighbour who thought he let too many men into his flat.] [I am] from Guinea. Police listened to the explanation of the neighbour and arrested [us].'*

Party raids and reports

Party raids have been among the **key police tactics** leading to arrest of LGBTQI+ people in Iran, according to our country-expert researcher:

> *The tactic is used indiscriminately for targeting queer and non-LGBTQI+ gatherings; however, LGBTQI+ individuals receive harsher treatment from police and security forces during these raids.*[21]

An interviewee from Iran stated:

> *'Sometimes the police come to the parties. With others (non-queer), it is very easy, and they release them on bail. But queer people are treated much worse. Insulting behaviour … it is so bad that my friends couldn't even share with me what happened. It is extremely traumatising for them, and they are treated in such bad ways that they cannot even recount the story.'*

On 16 November 2020 in Iran, some 40 armed plainclothes officers of the Ministry of Intelligence raided a garden party near Shiraz. The party organisers and most of the guests were members of the LGBTQI+ community. According to media reports, the officers were

informed about the party in advance and had laid a trap to arrest all guests. Some 120 guests were arrested during the raid. The officers handcuffed the guests and confiscated their mobile phones. The detainees were forced to provide officers with passwords to their mobile phones and those resisting were tortured. The officers did not show an arrest or inspection permit to the detainees. The caterers, the music band, and one of the guests were transferred to the police station for further questioning. The rest of the guests were released on the spot after interrogations and phone confiscations.

In interviews for this research, members of the LGBTQI+ community in Iran have tied the raids to online visibility of the LGBTQI+ community. An interviewee explained:

> *'Parties were regularly held in Shiraz and everyone was cautious to not post photos on social media. After one of these parties some participants posted pictures on Facebook and Instagram. The next party was raided.'*

Another Iran-based interviewee discussed parties and devices before people used them to store digital materials that could be used to 'incriminate' them (see also below):

> *'They took their electronic devices, but then it was not like now so they couldn't collect much from the phone as evidence. At that time, we had apps like Viber. But the videos that the guys had on their phones were very important to them.*

In Jordan, in early July 2021, police broke into a private party which was reportedly organised for – and by – members of the LGBTQI+ community. Little has been revealed; however, according to news reports, police knew of the event through monitoring public social media posts containing an invitation to the event.[22]

A similar party organised on Grindr was raided in Algeria where all of the attendees were arrested. Our interviewee managed to get off with a three-month prison sentence due to having an old phone with no 'evidence' on it. Others were sentenced to three years:

> *'Met someone on Grindr and went to a community party and the neighbours reported the party and [police] arrested everyone. Uniformed police. … Dozens of police officers came to the apartment and took us violently to the police station. I*

have never been so scared. … [We] arrived on site, no one knew anyone. We were all afraid. Some cried out their innocence … Sometimes, some took hits.'

Reporting combined with surveillance and monitoring

'To them, the digital world is a reflection of the real world. They exercise oppression there the same way they do in the physical world.'

– Jordanian interviewee

Under the umbrella of social surveillance and reporting is also the common theme of social media surveillance and monitoring – both by state actors/police and non-state actors who use it to enlist the threat or force of the police or state.

A new, concerning outcome from this research is the **vast use of social media monitoring – mostly by non-state actors – of queer people**, with 'social surveillance' used to report individuals to the authorities. On some occasions, this monitoring or social surveillance is used more as a threat to report or arrest than to actually report or arrest.

***16 out of 93** (17%) interviewees mentioned **experiencing social media surveillance and monitoring**.*

*Iran had **5 out of 16** – the highest percentage.*

Although this tactic was reported in every country of our research, Iran had the biggest percentage. With extensive surveillance systems in many of the countries, general surveillance of communication is not uncommon (see the Iran section in Part I).

Our country expert researcher for Iran outlined this in a report for this project:

LGBTQI+ individuals are harassed, threatened, and arrested in Iran daily, often after being surveilled on the apps and social platforms they use. Research findings and local experts' testimonials indicate that there is at least unofficial and random monitoring of apps used by LGBTQI+ persons. The use of the data gathered has

> *ranged from threats of arrest to use of the information 'incriminating' them under Iran's anti-LGBTQI+ laws when interrogating users for political or other activities seen as punishable by the state. Chat groups on Telegram have also been monitored, with LGBTQI+ groups having their admins arrested.*[23]

In Iran, cases ranged from university security monitoring social media and general social media monitoring by security forces to security forces' surveillance based on mistaken identity, informant-based social media surveillance arrests, and monitoring of tagged photos. The variations in all the types of surveillance and monitoring in the interviews processed for Iran show:

- They are all state related.
- There is a vast monitoring and surveillance system where the state wants the individuals to be aware they are being watched to ensure social and political control even if their intention is not arrest.

Monitoring cyberspace has been one of the key tactics used by Iranian police officers and security forces for identifying and targeting LGBTQI+ individuals. The security forces on various occasions have publicly acknowledged using the method. Data gathered through online surveillance has also been used for intimidating LGBTQI+ individuals into curbing their public visibility.[24]

For example, an Iranian queer woman interviewee who was arrested in 2009 during the Green Movement over attending political protests told us that intimate conversations with her then-girlfriend were used as an intimidation tool by Ministry of Intelligence officers during interrogations for political charges. The Islamic Republic's security apparatus has a history of intercepting SMS (text messaging) conversations and using the messages as evidence, especially against political dissidents and activists. The method was widely used against protesters in 2009.

In one case from Iran, the interviewee described the case of a person they knew although they did not know this person worked for the Iranian Ministry of Defence. The interviewee was arrested for throwing a queer party:

> *'One of the boys at the party was a foreign spy.'*

In this case, the 'foreign spy' did not speak Persian and was not Iranian but worked with the Iranian Ministry of Defence. His employers had been monitoring his activities. He was taken in for questioning where the extent of his monitoring and surveillance was revealed:

> *'They showed him the printout of his SMS. For example, the messages he [had] were with someone who would come to his house for a date. They showed him the messages that proved that he was gay.'*

The 'foreign' person in question was fired and asked to leave the country but was not prosecuted.

Although we have seen fewer cases of SMS monitoring recently – mostly due to the prevalent use of chat-based apps – we continue to see the monitoring of social media and other apps.

For example, we have WhatsApp and chat-based app monitoring documented in Iran. According to samples reviewed by us for this research, the SMS messages used by authorities that highlight WhatsApp monitoring follow two templates:

1. 'Your online behaviour has been deemed as infringements of specific articles of Islamic Penal Code [article numbers mentioned]. You are warned that unless you cease continuing and repeating the criminal offence you will be prosecuted. Centre for Countering Organised Cybercrimes.'

2. 'Your criminal behaviour of posting and reposting criminal content on cyberspace and specifically WhatsApp has been established. You will be prosecuted if you do not heed this warning and repeat the offence. Centre for Countering Organised Cybercrimes.'

Data gathered for this research indicates that the latter template has been used in more recent cases and mostly in conjunction with political and social protests.

An older incident from 2008 demonstrated general surveillance when people were taken into questioning by the Iranian Cyber Police (FATA) and the Centre for Countering

Organised Cybercrimes about a case with which they were wrongly associated. Regardless of the error, authorities showed them all their phone logs and Facebook comments for their 'investigation', which included the interviewee's friends and the people they spoke to and connected with the most:

> *'From the phone records, they understood we were close. They mostly mentioned comments and posts that we had left for each other on Facebook.'*

Most of the monitoring and surveillance cases we have seen in this research used traditional monitoring methods, through social engineering, such as fake accounts, rather than sophisticated surveillance. Still, more work needs to be done to identify methods used.

One Iranian interviewee was being monitored through their Instagram due to private artistic nude photos they had posted. They were sent warnings by FATA to confirm that they were being watched and to cite the laws they were violating. They clarified that the page was private with only around 90 followers; 80 of them were known to the individual and about 10 were semi-unknown. There were no hashtags used and no way for the page to have been viewed beyond the small circle of people. A fake monitoring account was therefore suspected to have been in that small list of people. They were sent a threatening message from FATA via SMS:

> *'Almost two months ago, I received an SMS from the FATA police saying that I had violated three laws. The first charge was promoting corruption and prostitution and the second and third charges were insulting the Prophet and insulting the government and the leader. The last two I think had something to do with my background and my family.'*

Naturally, they investigated the validity of the message and took precautionary actions that luckily worked:

> *'After this message, the first thing I did was to make sure it was authentic. The message did not have a number. It was not possible to fake it, it was sent from somewhere called the Cyber Police. I shared it with one of my friends who works in*

the field of cybersecurity. He told me that if I removed the posts and suspended the page, the issue would be resolved. I did as he said.'

Again, this interviewee spoke of constantly being in fear that they were being surveilled and were therefore censoring any and all of their activities online.

In June 2020, after several members of the Iranian LGBTQI+ community had participated in Instagram Live videos of famous Iranian influencers, they were summoned by security agencies. Officers threatened two individuals saying that they would face legal charges if they appeared in Instagram Live videos again. This highlights the level of ubiquitous monitoring those in Iran face, even on ephemeral live videos.

In Jordan, our country expert researchers report similar methods from June 2021, when an LGBTQI+ activist in Jordan reported being contacted by an informant on Instagram. The activist's account had posted rainbow flag graffiti in Amman prior to this contact. The activist was contacted by an anonymous online identity, and the presumed informant attempted to persuade them to reveal their identity following their graffiti work.[25]

Tagged photos have been an increasing issue and risk in at least **5 cases leading to arrests** in Egypt, Iran, and Tunisia (see below).

In Egypt, a case involved a posted photo from 2020 after the death of Sarah Hegazy. The interviewee posted in Sarah's memory and added a solidarity frame in their Facebook profile photo which was also in support of the queer community. This caused the interviewee to be reported by neighbours and surrounding circles. This led to them being

'[S]ubjected to a set of threats, including: murder, sexual assault with sharp instruments, rape, theft, and [also] reporting to the police that I am a homosexual activist and practising forbidden sexual relations and calling for spreading debauchery, insults, and slander.'

The individual then had to leave town, lost their job, and tried to get support for safety advice. They reached out to one of Egypt's LGBTQI+ organisations for this advice, which saved them:

> *'The organisation also advised me to close the concerned account temporarily after calibrating my photo and personal data on it. This advice helped me very much.'*

After returning to their original town, they were monitored physically and then arrested, after which they were made aware that they had been monitored online for their post.

In a party-related case, an Iranian interviewee pointed to monitoring and reporting as they had assumed the police were aware of the party due to social media monitoring and reporting:

> *'The police came to the garden and arrested [the attendees]. They took them to Khalili, but they didn't keep any of them very long. They kept them for two or three hours. They threatened and scared them, and there was a routine process that exists there to scare people. … Of course, they were arrested by the police, thank God it was not the work of intelligence services. That would have been much worse.'*

Out of all those arrested, one individual was subjected to the most abuse.

Like all the other cases, these events have led to a chilling effect whether online or offline. As one interviewee from Iran stated:

> *'Because of these arrests and being concerned about being monitored online, there is a constant feeling of insecurity.'*

In Algeria, apps like PlanetRomeo have been used for honey traps to threaten and extort individuals after social media and app monitoring. The issue of surveillance and monitoring touches on many methods of harm and arrest that we cannot fully cover in this current report. In one case in Algeria, one of our interviewee's colleagues at the university created a fake profile online and social engineered information out of the interviewee to prove she was a lesbian. He then reported her to campus authorities. She was taken to the university police and the police commissioner:

> *'The police officers on the scene took the phone … and quickly discovered that I was in a relationship with the other girl by reading our messages. So we were referred to the police commissioner [based on these text messages].'*

Our country experts in Tunisia have pointed out:

> *[A] form of brutality and harassment that the police use frequently is through social media. During the protests of January 2021, the police syndicate used their official Facebook page to out protesters who were from the LGBTQI+ community. They posted the faces of protesters alongside their IDs and used their dead names to shame them publicly. This led to many violent campaigns on social media and has also led to a lot of physical violence against the people that were outed.*[26]

Human Rights Watch also documented alleged police officers publicly harassing LGBTQI+ activists with social media posts, predominantly on Facebook, in January and February 2021 (see above).

In terms of monitoring on messaging apps, both in Morocco and Sudan, interviewees mentioned police on WhatsApp. One Moroccan interviewee explained:

> *'They access groups and you can't even spot them. A policeman I know was in a WhatsApp group without anyone knowing him as a police person.'*

In Sudan, one interviewee said that they were organising protest locations and were arrested because

> *'[T]here was a breach of one of the organisation groups on WhatsApp platform, and we found the security forces arriving before us at the site of the venue.'*

Security forces in Iran also routinely monitor WhatsApp and Telegram channels and have been known in the past to arrest admins and participants of LGBTQI+ Telegram channels.

Linked to this use of chat-based apps combined with other forms, one Tunisian interviewee explained that event invites, such as Google invites sent through chat-based apps like Telegram, can be monitored and accessed:

> *'Once upon a time, we had a Telegram group called Rainbow Zone. … A series of security incidents happened to this group, which over time made us close it down. For the birthday of one of the guys, we had put an RSVP on Google, the link of which was in this group chat. Someone had left threatening messages in that RSVP. We were worried that the police could show up and arrest us at a party.'*

In this case, this warning meant the individuals did not go to the party and remained safe.

The breadth and reach of monitoring are known by many of our interviewees and survey participants and are part of the reason why many take huge precautions online, especially on social media, or they censor themselves. The prevalence of monitoring on chat-based apps is less known or agreed upon, and thus many still freely communicate with some methods and tactics used for self-protection. This monitoring of chat-based communications requires more research and attention for safety precautions to be adequately placed by the community and platforms.

Monitoring and police corruption

Several respondents and interviewees highlighted cases of overt police corruption where police targeted them after being 'hired' by non-state actors. In these cases, an LGBTQI+ individual's details are provided to a corrupt police officer or security agent who – for a sum of money – identifies them and either uses the threat of arrest to abuse them for the individual who hired them or arrests them by using the powers granted to them through anti-LGBTQI+ laws.

In a concerning case of reporting and monitoring in Lebanon in 2021, our trans interviewee was being stalked and harassed on many platforms by a person in Jordan. The stalker was professing love for her and using her financial needs to gain access to her. Using the same method as in the other revenge cases, when she rejected these advances, the individual from Jordan reported her, and in turn her Syrian refugee friend, to the police as he announced: "I will not rest until I see you handcuffed even if I had to pay all my money." She found out their telephone lines had been monitored by police linking her to her refugee partner after they had been targeted, violated, abused, and then arrested by corrupt officers:

> *'It turns out the phone lines were monitored, and they knew where I was living from him. They entered the house, and what really bothered me was that I was only wearing lingerie, nothing under it – I was embarrassed.'*

They were humiliated, taunted, abused, and beaten, and their house was ruined:

> *'When they arrived they knocked down the door and entered by force then took my phone and hit me [took her and pushed her to the floor and attacked her]. … They took my money and vandalised my house.'*

She was arrested:

> *'In the car that was waiting to take me, I saw the guy who was with me, my friend, his face was filled with scars and punches. They brutally beat him up because he was Syrian.'*

The police had been bribed by the Jordanian individual. The proof was when one of the officers called him to show what they had done:

> *'He was video calling him and saying, "Look at her handcuffed." He was also saying: "See this fag, I handcuffed him for you."'*

The corruption of police in these cases is overtly apparent – further empowered by a system that rewards these abuses and arrests where LGBTQI+ people are seen as targets.

In a similar arrest of an individual in Tunisia who was a sex worker, a client did not pay them, and after a disagreement the client bribed the police to arrest them under false accusations of violence, after which their devices were searched:

> *'When we were arrested, they took my phone, looking for proof that I was gay. They hit us to make us give them our phones. They checked and took the photos they needed.'*

They were imprisoned, raped, and abused. Though the client was arrested with them, as he had bribed the police, his treatment was very different to that of our interviewee:

> *'He gave officers money. They were bringing him food, drinks, and coffees, and we, on the other hand, were handcuffed. … I was raped the first time in jail, by a guard. He wanted to have sex with me, but I refused, so he hit me, raped me. … They [gave] me four days in solitary.'*

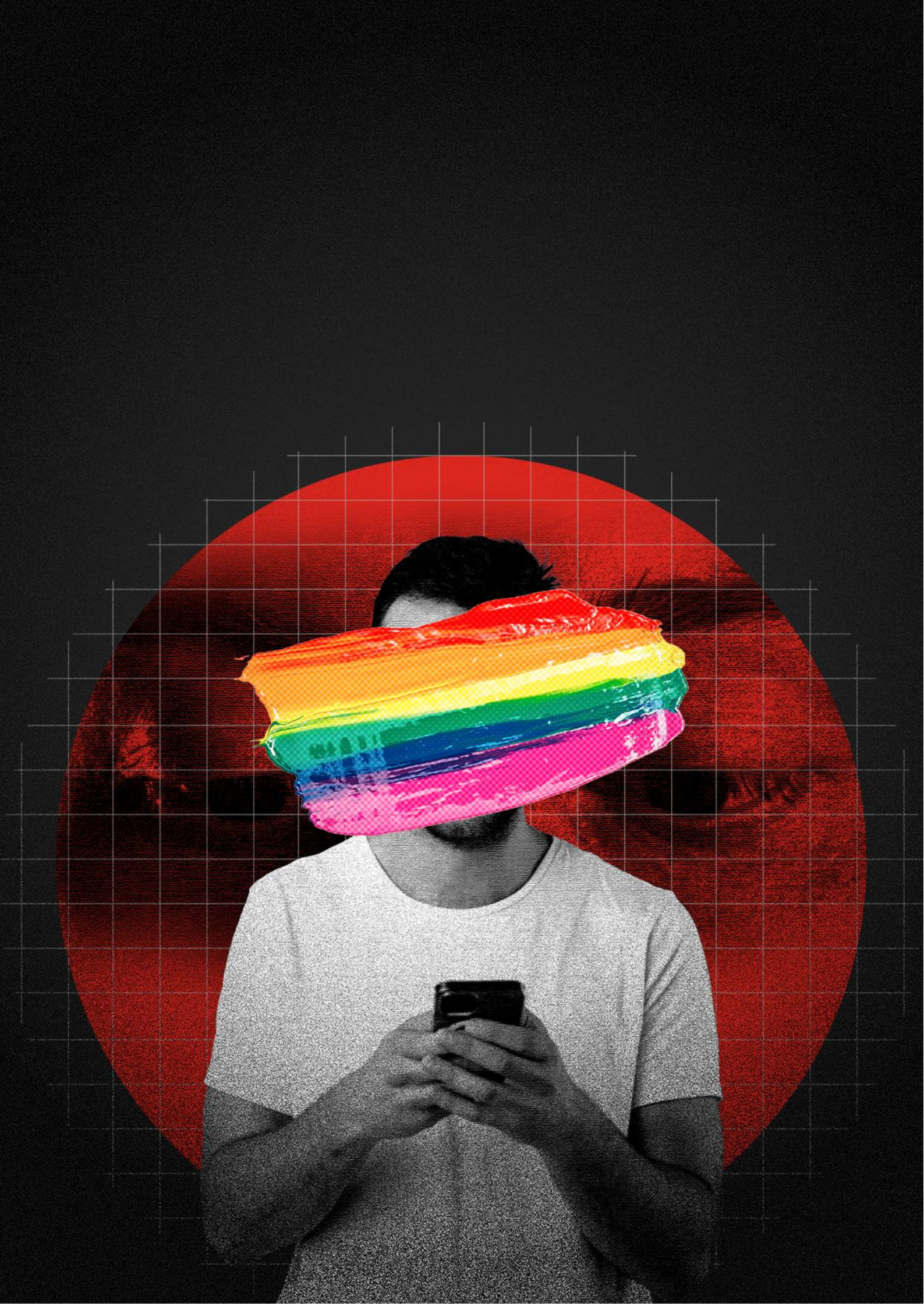
In a similar case in Tunisia, corrupt police arrested and violated a bisexual woman who was being targeted after their disgruntled boss had paid the police to arrest her and search her devices for queer content:

> *'I also found out that those who wanted to get my phone were paid by my previous boss to do so. I think they wanted to find pictures, because they asked me, "Do you like girls or not?" I was like, "What does this have to do with the reason I am here?" They said, "It's ok, we know you can tell us." Turns out the one who filed the complaint told them about me. … The people who were violent with me did not bring up the case … they just focused on my identity.'*

The new trend involving **police corruption and the use of technology** is to:

- Identify and frame the victims to peruse a device search for threats or arrest.
- Gather further 'incriminating evidence' on them to keep them in detention through what is found in the device searches.
- Have their 'crimes' documented for the people who hired them, presumably for full payment.

This revelation is one of the darkest sides of our investigation, showing how technology and our communication platforms have become interwoven with police and state corruption and abuse.



Device searches

Device searches are one of the most common and high-risk ways in which members of the LGBTQI+ community – like all criminalised communities – come under threat and are abused or prosecuted. The searches are almost always used and conducted against individuals or groups as soon as they are under the control of law enforcement. As previous research has shown, these searches are also often made **without warrants and/or without legality**, yet the **digital evidence from them is used in court** against individuals and/or for further information gathering, for social network surveillance, and/or as pretexts for abuse and violence.

The invasive methods used are outlined in this report, combined with how, miraculously, some have managed to save themselves from the consequences of device searches. The savviness of the community comes from the knowledge that in most, if not all, cases what is found on the device will either mean arrest and sentencing, or their release.

In our research, we saw the prevalence of this issue:

Interviews:	**47 of our 93** (50%) interviewees had experienced **device searches** in the 8 countries studied. This number is important, as nearly every interviewee who had had an altercation or interaction with the police and law enforcement in the previous cases had their devices searched or attempted forced access to devices.
Surveys:	Though we estimate the same high percentage of device searches with our survey respondents' experiences, we do not have an accurate number for device searches for survey respondents.
Focus groups:	In the 6 countries that had focus groups, device searches were also a very prominent issue, with every focus group having brought up the issue of device searches and forced access to devices.

In some cases, law enforcement uses illicit means such as 'jailbreaking' or 'rooting' or 'hacking' into phones to gain access to devices. This shows the levels policing systems go to in order to gain access to what they see as the 'digital crime scene' on the devices of the LGBTQI+ community.

On top of the issue of device searches itself, there are additional factors that add to the risks individuals face when being searched, such as the use of biometrics and phone numbers, which are important to study and create methods to combat. Forced access to devices (such as with threats and intimidation for passwords, violence for biometrics, or through jailbreaking or rooting) leads to further violence and prosecution based on the contents of the phones/apps that lead to outing queer content. Only in cases where people have denied providing passwords or acted drastically to get rid of their phones, have they been successful.

Features creating further risk in device searches

Biometrics on devices

One of the features that has created further risk and violence for our interviewees has been biometrics like Face ID or fingerprints to lock and unlock devices. These features have been used against them by the authorities to force individuals to open their devices. In this report's assessment and research, it can be confidently said that in general **biometrics locks are high risk and privacy intrusive, and in effect lead to further violence**. We do not cover privacy and the invasive and harmful nature of these technologies in general here due to the focus of the report, but rather how they empower abuses of police power.

---

7 out of 93 *(7%) interviewees had biometrics on their device enabled and had experienced being forced to open their devices via biometrics.*

In ***5 out of 7*** *(and thus the majority) of these cases, law enforcement used violence against the individuals to force the use of biometrics to open their devices.*

In this research, we see that the use of **biometrics has added risks of physical violence and force outside rules of law**. In every case where our interviewees or participants were in custody and had biometrics enabled – such as Face ID or fingerprint unlocking features – they were forced to access their device and did not have the option to navigate this demand. We also documented **5 cases that showed increased risk of violence when biometrics were enabled** on devices.

There is generally a low usage of biometrics to lock devices, which seems to be correlated with the distrust many reported having about the use of biometrics. However, the rate of violence used in the cases where individuals had biometrics enabled shows the increased risk of violence faced by those who do use the feature.

Like most of the risks and abuses outlined, this risk is also an international phenomenon. In the United States, for example, courts have long ruled that passwords are protected by the Fifth Amendment and thus you cannot be compelled to share them with the police without a specific warrant as they would be deemed 'testimonial' and 'self-incriminating'. Biometrics, such as Face ID and fingerprinting, do not have the same protections – and this has been an ongoing debate in the courts. The distinction relates to what is seen as testimonial, or revealing the contents of someone's mind, like a passcode. On the other hand, non-testimony, like Face ID and a fingerprint, are not part of someone's mind, but physical. Thus, the risk to individual privacy and rights is dramatically different when there is the introduction of biometrics instead of manual passwords and personal identification numbers (PINs).

Face ID and biometrics-enabled phones, in general, compel police to use physical violence to force access (e.g. grabbing someone's face or hands) with no option for refusal. Though similar issues can arise from passcodes, there is data and evidence that shows:

1. People are more likely to be able to refuse providing their passcodes and succeed.
2. People are more likely to have an ability to find ways to obfuscate giving passwords in critical contexts.
3. People have a higher chance to avoid physical violence and prosecution with passcodes than with biometrics.

For points 1 and 2, it is important to read the section of this report showing the lengths the community has gone to – and the stealth used – in order to avoid providing access to their devices, knowing that refusal can further 'incriminate' them. The risk of revealing the contents of their phones and risking the highest charges, as well as revealing their networks, is deemed higher than a non-compliance charge (see below). Some

interviewees also mentioned avoiding using these features in general due to their perceived safety and privacy risks. As one Iranian interviewee succinctly put it:

> *'I use PIN codes for all of them as I have been told that face recognition and fingerprints are not very secure.'*

One of our Lebanese interviewees described being forced to open their device with their fingerprint while handcuffed in 2022. They were beaten and provided no options for refusal:

> *'Immediately, when we arrived at the precinct I was handcuffed. He kicked me to the floor and asked me to open it. … He came close to me with the phone in his hand and forced me to place my fingerprint and open it. … They dove deep into my phone.'*

The same instance occurred in Egypt when the interviewee was handcuffed without any option for refusal or moving their hands, even though the individual had attempted refusal. This led to a lengthy prison sentence:

> *'We were detained in Somuah police station, and I refused to open my phone. … At that time, the officer handcuffed me with handcuffs and forced me to open the phone with my fingerprint, grabbing my hand.'*

In another similar case in Egypt, after our interviewee's friend's fingerprint was forced, 'incriminating data' was gathered on them and their friends:

> *'My buddies and iPhone had nude pictures of both of us, as well as sexual conversations on WhatsApp, Instagram, and the dating app (Badoo).'*

This led to their sentencing.

As another Lebanese interviewee outlined, her fingerprint was violently used to force access to her device despite her efforts to refuse. The content was then used to humiliate her. After the forced use of her fingerprints, immense abuse and the invasion of her privacy removed any chance of blocking access to this information and led to further violence:

> *'[Trans women have] private photos [on their phones]. I have private photos with my boyfriend, and my phone had photos of me in underwear. There is a video of me*

and my boyfriend in bed. They were watching the video and calling on each other, I swear by my mother's soul, that they were shamelessly watching the video.'

Jailbreaking/rooting or hacking phones

***4 out of 93** (4%) interviewees had experienced having their device forcefully accessed by law enforcement through the use of external technology after their arrest.*

Also importantly, and reflective of our previous research, individuals reported cases wherein, regardless of whether they provided access to their devices, the police used jailbreaking or rooting to access the contents of the devices. Although it is not clear if this method is systemic, it is a concerning trend that can be used against the community and against methods of self-protection.

For example, in Tunisia, one of our interviewees stated that the police had hacked into their device. It is unclear how this was done. Depending on the device, this is likely to be jailbreaking or rooting into phones using Israeli extraction technologies such as Cellebrite:

'I remember giving them my Facebook password, but it didn't work, so they hacked into my account … and checked everything.'

We also saw this in Morocco when a queer individual who was a police officer himself was outed after the Sofia Taloni incident. This influencer created a hate campaign by instructing her followers to find queer people on queer dating apps and out them, specifically providing instructions about the uses of Grindr. This individual was outed by the very specific notification sounds of Grindr in the police precinct along with colleagues he had been communicating with on the app. Later, as he reported:

'I found that my phone was hacked and the members of the commission had my discussions and my photos in disguise … [and they] found the applications and my photos and the photos I received from my friends. My phone was offline and locked and even [with that] they had access.'

It is likely that authorities were specifically using Cellebrite technologies or similar technologies as both Morocco and Tunisia have been documented as having large training programmes in the use of Cellebrite. This issue clearly requires further investigation.

These extraction methods were also previously documented in Egypt, Lebanon, and Tunisia. One Lebanese interviewee was threatened in 2021 with this method while detained when the investigator said:

> *'"If you don't open the phone we know how to open it. We will put you in a room on your own where you will rot."'*

One Lebanese trans interviewee experienced a situation where the authorities accessed her phone by connecting her phone to a laptop – one of the only cases we have where the individual was a witness to this forced access. Disturbingly, not only were they forcing access, but they also started to distribute the data they uncovered to other officers in further abuse of the detainee:

> *'They connected my phone to a laptop. I saw them. It happened before my eyes. They distributed the content on my phone when it was transferred to the laptop to each other. He was sending pictures of my ass and my breasts to his friends, in front of my eyes, to tease and hurt me. He sent photos and content via Bluetooth to his friends. He also stole the memory card. There are pictures of my late mother in one of the funeral halls.'*

Risk of using phone numbers

Interviews:	**12 out of 93** (13%) interviewees directly asked for a halt in the use of phone numbers as the main avenue to register and access social media and chat-based and dating apps due to risks to their safety and issues in access.
Surveys:	**1,472 out of 5,018** (28%) respondents to the relevant question said that phone numbers are the sign-up/login requirement that makes them feel the most unsafe. This was the highest picked option.
Focus groups:	Issues of real numbers were raised in all 6 focus groups.

Most messaging and dating apps still use SMS as a sign-up and login technique. Almost all major social media platforms rely on phone numbers and SMS for user authentication and account activation. While convenient and easy to use, SMS conversations and sign-up techniques endanger the privacy and safety of users in oppressive environments. The use of phone numbers has caused a lot of risks for the community. Authorities are able to link numbers to people's legal and official identity, leading to outing and prosecutions with digital evidence. They also create a discriminatory and access barrier for LGBTQI+ people in high-risk contexts such as Iran and Sudan who cannot use SMS and phone number verifications at all.

In Iran, recent reports revealed that phone numbers have been used to identify protesters since authorities are able to link to an individual's registered legal name and other identification number. There are hacking risks and risks that allow state actors to block access to services with the use of SMS for registration; however, that will not be covered in this report. Some of the ways phone numbers have heightened risks and increased the charges against individuals are discussed next.

Linking and identifying queer people and the issue of Truecaller

Mobile numbers are registered under national ID numbers in most countries, including those studied here. As a result, if an individual shares their number – or if they are communicating with someone on a chat-based app like WhatsApp or Signal – and their phone number is linked to the profile, it can be used to identify the identity and address of an individual, even if they had been relying on anonymity through an alias. This user discovery/phone number display is also often used in queer prosecutions as a method to link digital evidence – chats, photos, or videos – to the legal name of a person, thus solidifying a charge.

Methods such as screenshotting conversations with the sender's phone number linked to the account are often used in courts to create 'solid evidentiary' links between the communications and the individual's legal identity.

In the case file analysis from our previous reports, it was clear that even if individuals used fake names, the SIM card of an arrested individual would be used to match their phone number to conversations with informants or police. Having anonymity for users in these cases can be fundamental. In contrast, in a number of those cases, if the SIM card match

was not performed, the defence lawyers had an advantage when it came to disputing the evidence. The *Digital Crimes Scenes* report heavily documents this method.

This difference can be seen in the following case file extract from Egypt which was gathered in 2021 for the *Digital Crimes Scenes* report:

> In Case E4, the analysis to connect the number from the conversations with the entrapper to the individual is more advanced as the individual had also refused to provide access to the device. The case file states that the investigators used the Truecaller application to link the individual name to the phone number used.
>
> *Investigation notes:*
>
> 'When we opened the evidence number [redacted]; [it] contain[ed] a mobile phone, the accused denied knowing anything about this phone.
>
> When we searched for the sim card number [redacted] we found in the phone on "Truecaller" we found an account with the picture of the accused as a profile picture.
>
> It's also the most prominent pattern mentioned in the Egyptian interviews, where one lawyer explained that: "The most detrimental kind of evidence is mostly when the person switches from dating apps to social media, like WhatsApp and messengers, because these can be easily linked to the person's identity whether it is through the phone number and so on."
>
> The "practising habitual debauchery" charge is easier to dispose of in front of the judge, [because it] is harder to prove. … But if you are arrested with digital evidence like dating apps, or screenshots from the phone, or the phone number and so on, it is very easy for them to get you for promoting and advertising debauchery [Article 14].'

This is such a phenomenon that in the Egyptian focus group discussions for this research our participants explained that police have been using illicit ways to go on a quasi-illegal market in order to buy phone numbers of suspected LGBTQI+ people obtained by the 'informant'. They then use these phone numbers and other personal information to track queer people on social media and dating apps to arrest them, often through entrapment.

Truecaller reverse searches and phone number risks

One of the most prevalent new issues mentioned in relation to phone numbers and the link to real names has been the rise in use of Truecaller, as mentioned in the previous section. This issue was also documented in the *Digital Crimes Scenes* report, which details the use of Truecaller in even more contexts where Truecaller is used to out real identities and often home addresses. Truecaller is an app that advertises itself as providing caller identification and spam call blocking capabilities (none of these features have been verified for effectiveness or safety). The app also offers an invasive reverse number lookup that allows the user of the app to search and link a phone number to a registered name.

Apps and platforms collect the numbers and names of individuals on them, whether or not it is through informed consent. When users install Truecaller on their smartphone, the app asks permission to access their list of contacts to feed its own phonebook. Thus people's phone numbers will be saved solely if they were saved on a device that uses such a tool, without them agreeing to it.[27] The apps will also sometimes link to the social media accounts of users, as mentioned in the earlier case file where the prosecutors noted: 'When we searched for the sim card number [redacted] we found in the phone on "Truecaller" we found an account with the picture of the accused as a profile picture.'

Our participants and interviewees were aware of these risks and pointed to them as one of the ways they are put at risk by social media, dating apps, and chat-based apps. In our Tunisian focus group discussions, the participants discussed the lack of safety caused by the use and reliance on phone numbers by communication and dating platforms:

> *'As for dating apps, it is not safe at all to use, if you want to know data about me, like a phone number like they do now, how would I know that information will not be hacked or shared? People simply use Truecaller and identify who the person is.'*

Another interviewee in Tunisia noted:

> *'Some people can use your phone number on the Truecaller to find your real name and get some information they can use against you.'*

Interestingly, some community members have used this against the police – although this use is not common since police often use informants or obfuscated SIMs. We documented this in two cases.

A survey respondent explained how they both identified an officer and were put at risk because information like their phone number had been shared:

> *'I have a friend who got to know someone via Grindr, and he shared his photos and address with him, and before going to see him, he discovered that he was a detective through the Truecaller app. When he tried to avoid him, he threatened him, since he knows his address and how he looks. My friend had to change his phone number and address after this incident.'*

Phone numbers marginalise whole communities (Iran and Sudan)

In terms of accessibility, this registration method makes it impossible to use communication apps in places like Iran and Sudan.

Many of the most well-known communication and dating apps in Iran and Sudan exclusively allow registrations with text messages or phone numbers. However, some of these apps do not allow account creation with Iranian or Sudanese numbers (see below).

Some apps such as Tinder and OkCupid require a phone number for account registration but do not list Iran as a country and do not accept Iranian phone numbers, therefore effectively banning Iranian users.[28] It is a similar situation for the secure app Signal that many Iranians would rely on for safer communication. However, since it requires SMS registration and Iranian numbers are not recognised, Iranians have to rely on more unsafe options. One Iranian interviewee said:

> *'One of the problems with Signal is that it asks for a phone number, which is not necessary. Signal is a very good app, but I don't understand why it has this downside. Why not use an email address?'*

Individuals often become reliant on their networks outside of the country, or they need to exit the country themselves, in order to be able to access some communication apps. A

real divide is thus created between those who have resources outside of the country and those who do not. Highly vulnerable and disinvested communities do not have this access.

On top of the isolation and harm this situation creates in relation to the right to expression, it also encourages an already vulnerable population to revert to unsafe apps. Some users have turned to online temporary phone number services to register accounts on Tinder.[29] Some Iranians living abroad have started 'renting' their number to people inside Iran to create Tinder accounts. Both solutions pose security risks. An interviewee in Iran highlighted the toxic and exploitative nature this strategy has taken:

> *'A very hot market has been created where they sell phone numbers. Now they are selling foreign phone numbers that you use for Tinder. I can tell you the price range. This made me hate this app.'*

Searching devices and what authorities look for

Looking for proof of queerness

As we saw in our previous investigations, anything even hinting at queerness is seen as a crime and can lead to arrest. From romantic conversations and 'sexting' to kind or intimate messages to even just selfies.

In one Sudanese case, a very common and mild form of endearment was sufficient to start threats of arrest, violence, extortion, and abuse:

> *'They started searching my phone, I delete everything, so they didn't find anything. They found a message between me and the person I am with; he wrote "Habibi".'*

This simple and very common term of endearment was sufficient for the police to reach their conclusions and continue with their abuse:

> *'They said you are gays and you are the reason this country is wrecked. [They said] we will take you to check you medically [anal test] and then tell your families.'*

This type of data is used as digital evidence to support identity-based prosecutions. The need for digital evidence is especially acute because queerness and consensual sexual

acts rendered criminal under vague laws do not leave victims or crime scenes. Therefore, digital evidence becomes a key tool in providing evidence for a 'crime' that is otherwise very difficult to prove. It supports states in their efforts to criminalise an identity. Authorities use what is found on a device as 'proof' of queerness or 'crimes' and our research shows that, in many cases, they are searching specifically for evidence on devices for this 'crime' of queerness. They are looking for messages, photos, videos, and anything that hints – to them – at the sexual and gender identity of an individual.

In this section we discuss situations where police and the state are not just happening upon evidence but rather are looking for it in device searches. They may be looking for 'proof' of their charges and allegations of queerness. They may also be trying to coerce further confessions or identify others in the individual's networks.

For example, in Tunisia, one interviewee described this happening during their arrest. This mission for 'proof' meant the police looked over all parts of the device, often violently:

> *'When we were arrested, they took my phone, looking for a proof that I was gay, they hit us to make us give them our phones. They checked and took the photos they needed. They checked everything; they opened our conversations … they found pictures of me with my boyfriend.'*

Although this individual tried to deny the photos and 'evidence' discovered, due to the thorough search and broad access, the police found romantic photos with the individual's partner which were hard for the individual to deny, bearing in mind that Tunisian laws do not outlaw romance or intimacy. (For more on the prosecution of intimacy, friendliness, and queerness outside even the confines of the anti-LGBTQI+ laws, see this report.)

This use of identity and device searches for ammunition to build a case or gain further access to information and networks was also prominently mentioned in the Tunisia focus group:

> *'The police even took their phones and searched them. They ask to search your phone to intimidate you so that they can get more information from you.'*

A Lebanese interviewee recounted this relating to an arrest where the identity of her partner was being intimidated out of her:

> *'She was asking me, "Who is this?" and "Is she like you?" and "Where does she live," etc. I lied to her. I told her, "She lives outside Lebanon, she's in Canada, this is my mom" and so on.'*

Only this total denial saved this interviewee.

There are situations where police and state actors know the identity of individuals and then spend time surveilling, monitoring, or searching devices further. They often even regularly target and search individuals and communities until they find what they need. We have documented this method in Egypt, Jordan**,** Lebanon**,** Morocco, **and** Tunisia. For example, an interviewee who previously worked as a sex worker in Morocco told us about regular targeting and device searches, looking for evidence for extortion or arrest:

> *'I was a sex worker full time. Police people come often and check my phone in the corniche. They see if I have dating applications and nudes. If they find something they may take you to the police station if you do not tip them.'*

Another Moroccan interviewee reported this knowledge and prior evidence – or knowledge of queerness – being used directly to gain intelligence on the broader community:

> *'Once three policemen without uniform entered the house. They showed me photos and interrogated me for one hour. They asked for details about the LGBTQI+ community: what we are doing, where we meet, places and all the details. I tried to deny it, but they started threatening me. I told them many things about the community and where we met. I felt guilty about that. They freed me afterwards.'*

This tactic is used to **coerce individuals who are left with little choice but to become informants**, leading to arrests and further oppression of LGBTQI+ communities. A very common tactic police and state actors use against marginalised communities is to **maintain control through fear by gathering intelligence, accelerating arrests, and creating division and distrust**.

In this report's investigation, we have often seen that when police, investigators, or other state actors are looking to gain information on an individual, the likelihood of violence, abuse, and intimidation also increases.

For example, in Algeria, the police's violent pushes to gain access to this data and 'proof' translated to increased violence. Our interviewee and their partner were forced to confess despite their attempts to deny allegations and refuse a confession. This interrogation tactic led to their sentencing and the outing of the relationship of the two individuals:

> *'The head of the station was trying by all means to confirm the accusation of having sex on us, and he took the opportunity that my partner was afraid and started to intimidate him, knowing that we were separated and each of us was interrogated in a separate room by two different people. … Because of the pressures, and because the police accessed his phone where Grindr is installed, my partner admitted that he was in a relationship with me.'*

In another Algeria**n** case, the contents of the phone were again only accessed to 'prove' the individual's sexuality after subjecting our interviewee to abuse and torture:

> *'They started to examine [my phone] and read all my Facebook conversations and considered them as proof of my homosexuality.'*

This individual spent six months in prison based on these discoveries on Facebook Messenger and the forced confession.

In Egypt, the officers who knew of our interviewee's sexuality and their sex work used increased violence and humiliation to gain access to their device, especially after the individual refused:

> *'An officer with several police secretaries who arrested me asked me to open my personal phone. … He slapped me on the face in front of passers-by in the street, saying, "Oh, you're a bitch. You lick him." When I refused to give him my phone, they took me to the "morals" investigation in Sayeda Zineb. They entered me into a small dark room for two days, where I was locked up in solitary confinement. During the two days, I was beaten.*

> *I was sentenced to six months' imprisonment and six months' probation. They use digital evidence from my device. [They used] the conversations proving I'm gay and some nude pictures of me. They did not interrogate me about the digital evidence.'*

In Lebanon, officers used physical violence and other methods of torture. They handcuffed the group they had arrested and forced them to sleep on the floor for three days while berating them and threatening outlawed anal tests, all in order to gain access to their devices. This was an opportunistic arrest based on a drugs charge; however, sadistically, the officers knew about the gender and orientation of the individuals who were trans and wanted to gain further data on them to add a prostitution charge. After some time, due to having no available options other than refusal, our interviewee opened their phone:

> *'I was scared, as it was my first time in a police station. I opened the phone for him and he started looking into its contents. He saw my photos, he saw photos of me with someone hiding me. He told me: "Ok so you do actually get fucked." I'm in a romantic relationship.'*

After this incident, the threats continued to get worse as did the treatment of the individual.

Our Lebanese country experts reported that the Morals Protection Bureau of the Internal Security Forces, or the moral police station, has been avoiding using Article 534 of the Penal Code in some of the records.[30] Instead, they focus on proving sex work and/or the promotion or sharing of 'indecent' content, which in some cases was 'proven' by porn history saved in search engines history.[31]

In Algeria, one of our interviewees described the same type of situation when a violent interrogation was finalised with device searches and the interrogator's confirmation of their identity. The interrogator's only intent was to prove their hypothesis of the individuals' identity:

> *'At first, the interrogation relied solely on verbal abuse. Then they took my phone and asked me to enter the password to open it using physical violence. … They started to examine it and read all my Facebook conversations and considered them*

as proof of my homosexuality … especially since these conversations contain my nude photos and videos.'

In our Algerian focus group discussion, a case not related to state actors shows the power and harm this knowledge, combined with evidence from a person's digital devices and profiles, can have. Even in the midst of blanket immunity for criminalisation and abuses against LGBTQI+ people, **these tactics can be used for long-term violence and extortion**. This individual was raped and abused for three months leading not only to the traumatic impact of this violence but also to the loss of their position at university:

'One day, four students, two of whom live in the room next door, violently entered my room, took out my mobile phone and ordered me to open my Grindr application with my PIN code. At first, I resisted but they were very violent and I finally gave in. They discovered my nude photos and others where I was in sexual situations with men.

They photographed these photos with their mobile phones and then forced me to have sex with each of them.

Since then and for three months, they forced me to have sex with them and other friends of theirs and threatened to release my photos if I refused. Those three months were the worst of my life, I suffered physically because they raped me violently and repeatedly and I lived in terror that my photos would reach my family. I ended up leaving the university residence because I couldn't take it anymore.'

There is also a history of this in Iran:

Coercing LGBTQ individuals – arrested in LGBTQ-related cases or parallel cases – into working as informants has been among the tactics used by police and security forces in Iran. The method has been used as recently as June 2020 when Iran morality police arrested a transgender woman and tried to coerce her into working as an informant. The officers sought information about LGBTQ gatherings.[32]

In Sudan, device searches are very common and have been throughout the turbulent crisis and wars. Despite being the most rapidly shifting and militarily controlled of our research

countries, our Sudanese interviewees have shown impressive tact in avoiding searches (see below). This is exacerbated by the political risks in the country. For example, the African Freedom of Expression Exchange has reported that in October 2021 the military forces that staged the coup had legal provisions available to them to search individuals' phones and to delete documentation of human rights violations that were perpetrated.

Contents of devices outing individuals

In other cases, in fact in most cases, the contents of devices themselves outed individuals and put them further at risk. When a device comes into the hands of police, their searches can lead to data being discovered that, in their minds, reveals the identity of an individual, which leads to further interrogation, arrest, and general abuse. This can happen during opportunistic arrests, when another crime is being investigated and an individual's gender and sexual identity is discovered due to the contents of a device. It can also happen if an individual is profiled on the street and has their device searched for any reason. But it can also happen when an individual has lost their device and the device is handed over to authorities. All these different scenarios dictate and exemplify how simply encountering authorities, which can lead to access to a device, constitutes major risks and threats for the queer community.

***18 out of 93** (20%) of the interviewees from all 8 countries who reported arrests to us stated that their identity had been discovered after the content of their devices was seen.*

In several cases reported to us, individuals who were making reports to the police or under investigation for unrelated crimes were then mistreated or charged for their identity due to the discovery of the contents of their devices – especially in Lebanon**,** Morocco, and Tunisia (see above).

In a street arrest case in Morocco, not only did police arrest the individual after discovering their identity through searching their phone, but they also outed the individual to their family:

> *'They caught me. They took and searched my phone. They found my nude photos. They arrested me for 48 hours and called my mother. They told her that "your son is gay". They outed me.'*

In Egypt, this outing from a device search led to the six-month prison sentencing of one of our interviewees. They found 'incriminating evidence' sufficient to gain this sentence in the court procedures:

> *'Grindr conversations and nude pictures of me. They interrogated me about the digital evidence. They forced me to unlock my phone and I was already logging in my accounts. … Based on the dating apps on my phone and the conversations they contain, I was convicted of practising debauchery and inciting it, and I was sentenced to spend six months in prison.'*

One of our Egyptian survey respondents explained a similar situation where, after a device search, the discovery of Grindr led to the person's prison sentence:

> *'One of my friends was arrested last year in Egypt because he had Grindr on his phone, so he was beaten, insulted, and bullied by the Egyptian police. He was imprisoned for six months, then charges such as debauchery and practising vice were brought.'*

In another Egyptian case from one of our interviewees, we see this play out when the individual lost their device and had to go to the police department that had found the device to prove ownership:

> *'[The police department officer] asked me to unlock it using the password to make sure that it was really mine, even though I brought the phone box and the bill with me, but the officer insisted that I open it. I had forgotten at the time that the background that I was putting on the phone was a snapshot from the Elite series of two gay people kissing.*
>
> *The officer asked me what it was, and I replied that it was a regular clip from a series, and he started searching my phone further.'*

The only saving factor here was that the individual had used app-cloaking and other obfuscation methods to block access to the potentially 'incriminating data' and apps on their device.

In Iran, device searches, confiscations, and inspections have become more frequent in the Islamic Republic in general. Many of our interviewees outlined searches at political protests and being stopped by the morality police and state-backed militia Basij for their claimed non-adherence to the strict hijab laws. These searches did not lead to the outing of our interviewees by sheer luck, but our interviewees outlined the risk they were under when such searches occurred.

What the police/state are looking for in device searches

Everything

Interviews:	**7 out of 93** (7%) interviewees mentioned how the police had looked through 'everything' on their device in their search.
Focus groups:	Participants in Tunisia and Morocco mentioned how the police had looked through 'everything' on their device in their search.

In our investigations we saw that, for device searches, the police, interrogators, or other state actors looked through specific parts of the devices, often to preserve time. But depending on the skills, resources, zeal, and capacity of the authorities, they can also just look at the device in general. One of our Tunisian interviewees said:

> *'They had a tool to open my phone … they went through everything.'*

Another Tunisian interviewee had the same experience after physical violence:

> *'When we were arrested, they took my phone, looking for proof that I was gay … they checked everything.'*

In Jordan, one interviewee, who was also an advocate for arrestees, explained the time taken to browse through phones in these instances. The most popular platforms and apps were the most searched:

> *'All of their social media – which the usual suspects are Facebook Messenger, Facebook, applications like Grindr, applications like Tinder, pictures and videos that they have saved on the phone. … Text messages on the phone, whether on WhatsApp or actual SMS and other you know, like, communication apps.*
>
> *They take time. They take their phones for a while and then bring them back after.'*

In Egypt one of our interviewees described a search as the 'trifecta' of dating apps, social media, and messenger apps in order to push evidence-gathering beyond the use of photos from the camera roll:

> *'In my arrest case the police officer used the conversations on my WhatsApp, Instagram and Badoo gay dating app (sexting) as evidence to file a case for me and four of my friends who were with me on that day. The police officer also forcibly accessed my phone gallery that contained naked shots of me.'*

These are examples of the most common format – when police have easy access to data which allows them to compile evidence unchallenged. In such cases, safety on the phone and its operating system is vital (see Part III).

Device contacts lists

Another new, concerning pattern we saw in this research is the use of contact lists and contacts on phones in general by the authorities.

***7 out of 93** (8%) interviewees explained how, during device searches and inspections, officers called people on their contact lists or in their messages to gain more information.*

Often, they looked for particular contacts such as people's parents or simply the last people with whom they communicated. They use their phones to call them or in some cases message them to further 'incriminate' the individual and others in their network.

In one interview with a Lebanese trans sex worker, she outlined how the police had tried to implicate her in crimes by messaging her contacts, but as our interviewee cannot read or write, her contacts knew this was a trap:

> *'They spoke to [messaged] people and claimed they were me. But no one believed them because everyone knows I am illiterate. I don't know how to read or write. [They wanted] to implicate them and me. My charge was small, they wanted to exaggerate it.'*

The same Lebanese interviewee was stripped and subjected to hate speech and abuse. The police continued this intimidation and abuse by calling her family in an attempt to trap her sister and brother-in-law:

> *'They were searching the [contacts] and calling a lot of people on my phone list. … They asked me about people. Who is this, and who is that? … They searched all the apps.*
>
> *They spoke to her [the sister's] husband. They started talking to him, and they sent him pictures of me wearing make-up. I am a transsexual, I respect my brother-in-law's opinions, and people's opinions in general.'*

Similarly, in Morocco a device's contact list was used for intimidation and outing our interviewee to their parents. This same method was used in another Lebanese case against a group of trans women, including our interviewee, who were arrested. The numbers extracted were kept as a threat against them:

> *'They took all the phone numbers. They called everyone on the phone list. They called their parents. … They were warned that any wrong behaviour will put them at risk of being imprisoned again. They also extracted their friends' and families' phone numbers.'*

In Sudan, during a street shake-down, officers removed our interviewee's SIM card to gain access to their contacts and they threatened to call their families, but it was intended only to extort from our interviewee:

> *'They took out the chip after the threats that they called our families. He was satisfied with the phone and the money. I was very careful that they threw away the SIM card, so the name will not show up when searched, and they did thanks to God.'*

This issue with SIM cards leads to the outing of names and is unfortunately a common issue (see above).

This method failed with one of our Tunisian interviewees who had the foresight to know about these methods and obfuscated the names of contacts on their phone:

> *'They asked for my mother's number. I didn't give it and they didn't find it, because she is saved with her nickname, not her name or "mother" or something like that so people won't know she is my mum.'*

In this case, we see how savvy obfuscation methods either through the device, or through personal safety measures, can save people from outing, further implication in crimes, and other societal abuse and harms.

Images: the visceral

***17 out of 93** (18%) interviewees mentioned use of photos and videos against them after a device search. In **10** of these cases, the photos were used as evidence against them in court cases or for adding additional charges.*

Perhaps one of the most searched and most detrimental forms of digital evidence for a case are photos and videos, due to their visceral impact and the difficulty of challenging their authenticity. Thirteen of our interviewees who had been arrested directly mentioned the search and identification of photos on their devices, either from the galleries of the devices or collected from chats within different apps. Four other interviewees also mentioned videos.

Photos, for the police, investigators, and other state actors, are seen as 'hard evidence' and proof of sexuality. Photos or videos of individuals engaged in intimate acts that are

considered to be criminal by the prosecution teams are the most damaging. In 10 of these cases, the photos were used as evidence against them in court cases or for adding additional charges. In some cases, only the photos or the videos are used – sometimes only one visceral form of evidence is needed.

The harm of these images was exemplified by one of our Algerian interviewees:

> *'Then they took his phone and asked him to enter the password to open it using physical violence. … They started to examine him and … considered them as proof of his homosexuality … especially since these conversations contain his nude photos and videos.'*

An Iranian interviewee explained how, after a raid of a party, in the authorities' interrogation and gathering of digital evidence from their devices, only the videos were used from their phones:

> *'The videos on their mobile phones were used as evidence against us, but the information on the messaging apps was not used.'*

Although it is not accurate to say the omission of 'incriminating messages' and other types of data is common, it does testify to the risks visceral images can create.

In other cases, authorities are looking for these photos so they can verbally abuse and/or use these photos and videos to either gain a confession or implicate people in other crimes. One of our Lebanese interviewees said:

> *'They asked me about people. Who is this, and who is that? They saw private photos of me and asked about them. They asked me to whom I sent them. They started asking me, "Are you in a prostitution network?"'*

We heard about this situation in many of our Lebanese interviews. Trans women were some of the most affected (for example, see the testimonies above).

Another of our Lebanese interviewees broke down in tears explaining how the officers had humiliated and harmed her through the search and questioning of her photos:

> *'If they saw someone's photo on my phone, like the photo they saw of my brother, and he is dead, and they asked me: "Who is this? He fucks you?" [Cries on the phone] Imagine this moment. This is too much, you know?'*

Furthermore, it was not only in interrogation after arrests that these incidents occurred. One of the most common times when photos and videos were searched was during street-based stop-and-searches. For example, in Iran a few interviewees mentioned how the individual was stopped due to hijab-based charges:

> *'The officers checked all the photos on her phone. They even made comments like, "You look very good in this one."'*

Conversations and chat applications

***13 out of 93** (14%) interviewees mentioned use of their messages and conversations against them by law enforcement after device searches.*

After the damaging effect of photos and videos – especially those seen as queer or with clear romantic or intimate content – conversations were heavily searched for and used by the authorities. Thirteen of our interviewees mentioned access to messages on their devices that led to further 'criminalisation'. Oftentimes the messages – and conversations in them – contained exchanges of videos and photos, linking to the risks outlined earlier. Here the police, prosecutors, or state security read through conversations and utilised the 'search' option in the chat-based apps to find specific words or conversations that could be 'incriminating'.

The applications that were most mentioned were WhatsApp, Telegram, and Facebook Messenger. These were the most commonly used applications for chats and conversations and thus the most immediately accessed by police and investigators when they were in contact with devices of arrestees.

An Algerian interviewee was sentenced solely based on the information found in his conversations with an individual and was sentenced to six months in prison 'because the police accessed his Messenger chats and they took this as proof of homosexuality'.

Of course, when the conversations included photos and videos, they became the most damaging because they linked the evidence and 'intent'. Numerous Egyptian interviewees mentioned the use of conversations from chat-based apps and dating apps to be the reason for their sentencing and charges:

> *'Yes, they found the conversations on Grindr and WhatsApp – which indicate the intention of sexual practice and sex work on that day. … They use them in the interrogation process as digital evidence.'*

In Algeria, searching directly for messages outed one interviewee and her relationship and provided proof the police needed.

However, in other cases, messages were used – similarly to videos and photos – to attach charges or accusations onto the individuals. As one of our Lebanese interviewees said:

> *'When they checked my phone they accessed Messenger and took it as an excuse to throw accusations on me.'*

In one particular Egyptian case, the interviewee had in fact followed all of the safety protocols. However, while having their device searched on a street-based stop-and- search, a notification of a message on WhatsApp popped up with an explicit message. They were detained and subjected to violence and abuse, which meant that though they would have otherwise been let go, they were outed and arrested.

Dating apps

10 out of 93 *(11%) interviewees directly mentioned the use of dating apps against them by police during their device searches.*

Dating apps have special importance because they connect queer communities and represent the most intimate and fragile interactions with technology. They are used to meet, to have community, to hook up, and to fall in love. For law enforcement in these contexts, being on a queer dating app is in itself proof of publicly pronouncing one's sexuality. This practice is well documented in Egypt and also in Lebanon and Tunisia and the broader region. The use of LGBTQI+-specific platforms, such as Grindr, PlanetRomeo, Badoo, Hornet, SCRUFF, Wapa, and HER, as mediums for connection, has risen dramatically in recent years. There is also a wide variety of apps that are used both by the community and by police to identify people. The most commonly used apps by our participants were Grindr, Hornet, Badoo, and Tinder.

The very presence of one of these apps on a phone was seen as a sufficient reason for arrest and additional charges. Unlike chat-based apps, there was no need to rifle through the messages – the app itself was often evidence. Apps like Tinder, however, can function like chat-based apps wherein the search of the app is required to conjure up any 'criminal' activity – unless the individual has indicated their identity on their profile. However, we see in our research that apps like Tinder have increasingly been searched, and our interviewees and participants noted that they have more queer conversations on them. Naturally, as this is a dating application, their sexuality was easily identifiable. Yet, the presence of Tinder on a device may not elicit suspicion.

Our country expert partners in Sudan noted that, during the current devastating war, there has been increasing risk and the rise of app infiltration by the paramilitary Rapid Support Forces:

> *In today's digitised world, online platforms play a crucial role in fostering and upholding connections. However, these platforms are not without their risks. Reports suggesting RSF's [Rapid Support Forces] infiltration into dating apps convert these digital havens into potential minefields for queer individuals. The lurking danger of exposure or targeting restricts many from accessing these platforms, further limiting their safe spaces. Lastly, while the highlighted narratives underscore the distinct challenges confronting the queer community, it's imperative to note their shared experiences with the wider Sudanese populace.*

> *Tales, such as a queer person jeopardising their life to help another, serve as potent reminders of the collective dreams, pains, and hopes for a tranquil Sudan, transcending sexual orientation.*[33]

This sentiment was reflected by one of our interviewees, with whom we conducted a short interview since the outbreak of war in Sudan:

> *'The Rapid Support Forces have been prevalent on dating apps during this period, which wasn't the case before the war. This deterred queer individuals from using these platforms due to fear of the Rapid Support Forces. Mentally, I felt scattered and exhausted; dating platforms weren't my refuge that would help in these difficult times.'*

In the interview with one of our Algerian interviewees, it was the presence of Grindr on the phone of our interviewee's partner that led to a confession about their relationship in the interrogation. It led to their sentencing.

One Egyptian interviewee was given six months in prison based on their Grindr app and its contents, which included conversations, photos, and videos:

> *'[They found] Grindr conversations and nude pictures of me. They interrogated me about the digital evidence. They forced me to unlock my phone and I was already logging in my accounts. … They searched my phone in the presence of the section officer, and the next day I was transferred to the prosecution. … Based on the dating apps on my phone and the conversations they contain, I was convicted of practising debauchery and inciting it, and I was sentenced to spend six months in prison.'*

The fact that this individual had no passwords protecting their apps was detrimental in this case with no avenue for them to deny or obfuscate access.

In other cases, the notification sounds of particular dating apps which are distinctive have led to outing and further searches, as seen in Lebanon **and** Morocco, and in Egypt especially:

> *'One time, I was sitting with friends and I received a notification. I forgot to remove the app, honestly. … When I received that notification one of my friends looked at me and was altered. He didn't say anything. He went to my friends and told them. They started offending me. They were saying: "You are gay", "You are a faggot", "Turns out you are dirty."'*

It is important to note that due to both the risks dating apps pose and the increased safety features available on these apps, people have been taking more safety precautions on them: from deleting their dating apps or using the app-cloaking options to hide their apps or installing passwords. These tactics have been the difference between sentencing and being released (see below).

Our Tunisian country experts outlined why taking measures so that people can verify, communicate, and connect more safely were vital:

> *Because of the general homophobic atmosphere in Tunisia, most app users do not include a lot of information in their profiles to reinforce their security. However, that plays to their disadvantage because the people they interact with are sharing very minimally also and usually providing false information on their profiles. This usually leads to the parties meeting each other in a private space which could lead to several types of abuse.*[34]

Social media accounts

Social media posts have led to the arrests, monitoring, and targeting of many of our interviewees. Many examples of this can be seen above. In our interviews, we had **16 cases of social media surveillance and monitoring** in all of the research countries. Iran had **5 out of 16 and the biggest percentage**. These included cases of posting photos of parties, solidarity campaigns, any photos with a link to queerness, liked pages, friends lists, and tagged photos – and it was especially the case for Facebook and Instagram. We also had reports through our interviews and focus groups about how the lack of privacy on event invite pages has outed large numbers of the LGBTQI+ community.

We have also seen increasing use of fake profiles on not only dating apps but also social media such as Facebook and Instagram to entrap and target individuals. For example, in

Algeria, Egypt, and Tunisia, there have been cases where dating apps have been used for honey traps, only after social media and app monitoring. Then come the meet and threats to extort from individuals (see above). In other cases, a person's Facebook profile has been monitored, and then fake profile conversations were started on Facebook Messenger leading to outings, arrests, and entrapment.

As mentioned, police use of social media to surveil queer individuals has been prevalent, especially in Tunisia (which was previously documented). More recently, this has been used to target queer protesters during the protests of January 2021, where the police syndicate used their official Facebook page to out protesters from the LGBTQI+ community. These tactics included posting their Face IDs and using their dead names to shame them publicly and doxx them. This led to many violent campaigns on social media and has also led to a lot of physical violence against the people who were outed.[35]

In places like Egypt, Iran, and Morocco, 'Lives' on Instagram and Facebook, especially, have been used by both state and non-state actors to identify participants and arrest and out them, endangering their lives. The ephemeral nature of 'Lives' has been used to bypass platform accountability and gather hundreds and thousands of views without leaving a longer-term trace. Outing campaigns, and campaigns pushing for violence against the community, have seen an increase in places such as Egypt and Morocco. Those partaking in 'Lives' have also been targeted when these pages were – unbeknown to the owners – monitored. In June 2020, after several members of the Iranian LGBTQI+ community participated in Instagram Live videos of famous Iranian influencers, they were summonsed by security agencies.

General access and the lack of privacy between who can see the photos and what is revealed through the 'recommendations' and account 'feed' on the 'actions' of an individual have led to the outing and even arrest of individuals. Many of these cases are included in numerous parts of this report and form part of the basis of the recommendations in Part III.

For example, in the case of an Egyptian interviewee, the Facebook post of an individual was the prime element in the case being built against them in their arrest. Luckily, the only reason they were not charged and imprisoned was that – based on the recommendation

of the LGBTQI+ NGO in Egypt – the individual had created a new Facebook account before encountering the police. They made this move after receiving intense threats and were reported for making a social media post in remembrance of Sarah Hegazy. They denied connection to the account they were reported for, and the account was not found on their device as they had a new 'clean' account.

Outing campaigns from state and non-state actors using data from social media profiles are highly prevalent, as documented throughout this report. Several of our interviewees who had experienced device searches mentioned the use of their social media. In these cases, it was often their tagged photos or private messages that were reviewed.

***5 out of all** our interviewees directly mentioned tagged photos leading to their arrest.*

In Tunisia, one of our interviewees mentioned that they were accused of being part of the protests and linked to the queer activist Rania Amdouni due to a tagged photo:

> *'Turned out they checked Rania Amdouni's Facebook profile, they found a post she posted and tagged out names in it, every single person that was tagged in that post was part of this case.'*

The case included a queer friend who was summoned to court, even though they were not in Tunisia at the time of the protest.

In other cases, stories, as well as the traditional use of posts or liked pages, have caused risks for arrests and evidence. In an Iranian party case, an individual was arrested due to tagged photos on Facebook and Instagram.

How the community has been outsmarting device searches

An important finding through this research was the community's response and resilience to these invasive procedures. It was no surprise that all those involved in this research were aware of the risks that the content of their phone brought for them. In many cases, our participants and interviewees reported taking high risks and drastic measures to avoid providing access to their devices, even if this action resulted in further physical abuse or incrimination. In these specific cases, they often weighed the risks and decided that there was a higher risk of 'incrimination' if their devices were to be searched than not – not to mention the risk to their community and network. See Part III.

On top of taking these risks, others used harm reduction methods, either from their own ingenuity or with the help of safety features provided to them.

In our surveys, we asked our participants about the features they used to provide safety for themselves. We specifically focused on safety features we had worked on with partnering companies. Out of the features that ARTICLE 19 pushed to implement on dating apps:

---

600 out of 2,264 *(26%) respondents said they use 'media and chat deletion, and disappearing messages'*

191 out of 2,264 *(8%) respondents used 'unsend' messages. Both categories fall under ephemeral messaging.*

We view these features under the umbrella of **'ephemeral messaging'**, and our survey shows a large percentage of respondents rely on them for their safety.

Ephemeral messaging features are available on some dating apps and a number of chat-based apps. This optionality has always been highly requested and relied upon by the community, as we have seen and recommended in previous work.

The next most used feature is **'app cloaking'** or discreet app icons on Grindr (also now available on the Android version of the Signal App, with App Icon changes introduced as part of a collaboration with Design From the Margins and this work). Despite the limited number of apps and platforms that provide this option, it was still one of the most relied upon features mentioned.

PINs and **screenshot blocking** were also some of the most mentioned features, with **63 respondents** mentioning these features. While these features were often mentioned, they are only available on very few specific apps, showing the reliance on them despite their limited availability.

***212 out of 2,264** (9%) respondents reported relying on 'all features' to protect themselves. This response was the third highest.*

Finally, the 9% of respondents who said they used 'all features' show that our respondents used all the specifically mentioned features, i.e. ephemeral and unsend messages and photos, app cloaking, PINs, and screenshot blocking, for their safety on these apps (not including options mentioned in their open textbox response option).

These responses show the prevalent use of these tactics by our interviewees and survey respondents in order to obfuscate and reduce the amount of data available on their devices.

In a separate survey question about the general methods people used to protect themselves (without being provided with specific options in relation to dating apps or features we helped introduce), **2,239 out of 5,018 (45%) respondents mentioned app cloaking**.[36] A more widespread take on methods used can be taken from this question as this was one of the questions in our surveys where all 5,018 participants responded to the question.

2,239 out of 5,018 *(45%) survey respondents reported relying on app icon 'cloaking' or obfuscation features to protect themselves when asked about general methods people used to protect themselves (without being provided with specific options in relation to dating apps or features we helped introduce). This response was the highest response.*

In the same question as the one mentioned above in relation to the general methods people used to protect themselves (without being provided with specific options in relation to dating apps or features we helped introduce), the second option was simply deleting all their apps (1,645 [33%] respondents). The third option was using 'fake names' or anonymity (1,508 [30%] respondents), and the fourth option was using timed and unsend messages (1,475 [29%] respondents). This finding is huge and demonstrates the desire for – and use of – safety features created with communities at risk in mind alongside the older safety method of just deleting or removing all apps, which is increasingly impractical.

In the survey, an overwhelming majority of 59% (2,430 out of 4,128 respondents) said 'yes' on whether these features determined their use of apps and platforms, with 34% responding 'I don't know' and only 7% saying 'no' out of the 4,128 respondents who responded to that question.

Risks taken to avoid providing access to devices

15 out of 93 *(16%) interviewees took extreme or dangerous measures to avoid providing law enforcement access to their devices, with* ***6*** *only in Sudan.*

There was a higher risk of 'incrimination' and harm to people and their network and community at large if their devices were searched than if they provided access in the first place. This finding is an important one because it shows that actions taken to block unauthorised access to devices, or ensuring that individuals have methods to wipe

devices, are fundamentally important as a harm reduction tactic. These methods will support tactics people are already taking.

For example, **15 interviewees reported taking measures to avoid giving access to their devices**. Methods included breaking their phones, hiding their devices, vehemently refusing to give their passcodes, claiming they did not remember their passcodes, or in a few cases, using technological tools to wipe their phones before providing access.

One Tunisian interviewee was already exposed both legally and physically, but they wanted to reduce the amount of information accessed by the police, so they took drastic measures:

> *'[When] they left my phone on the table, I broke it so that they wouldn't be able to see anything more.'*

Again, this pattern of **'by any means necessary' was much more prevalent than in our previous investigations**, which was potentially due to the **police's increased reliance on digital evidence** for prosecutions and using devices as 'digital crime scenes'. Those arrested have taken it upon themselves to block access to their content by any means necessary because they know how detrimental a device's contents can become.

In Lebanon, trans interviewees faced the most violence and intimidation and were also the most likely to take drastic measures to avoid giving sensitive details. One interviewee recounted refusing to provide passwords and access to their device despite being faced with threats of violence and rape:

> *'He asked me to open the phone several times. I refused asserting that I had private matters on my phone … [then] to threaten me he said: "Open it, or else I will take you to the barracks, and let everyone fuck you." I told him: "Do whatever you want. I will not insert the passcode and the phone will stay closed."'*

After this abuse and threats of violence, the individual obliged but took measures to reduce the potential exposure by limiting the access to the phone to five minutes:

> *'When they took the phone, they asked me to open it. So I accessed the settings immediately and made sure that the phone would close in five minutes automatically.'*

Another Lebanese interviewee faced similar violence and threats:

> *'I told him it wasn't his business and that I can't open my phone because it has photos of my brothers and my veiled sisters. He started threatening me where he said he would give me a test to confirm I was "alright". I answered that I don't care about the test he will do and that I am not interested in it and ready. He meant "a test down there" [anal test].'*

Sudan's interviews showed the most drastic and sophisticated methods. Our interviewees have been incredibly savvy, with **6 interviewees (largest number)** using drastic methods to avoid providing access to their devices. One interviewee outlined separate instances of arrests and device searches:

> *'In both cases, they took my phone … in both arrests, I refused to cooperate in opening the phone.'*

The interviewee went on to explain:

> *'[he] first time I broke the phone screen, it became difficult [for them] to access it, and the second time I claimed that the phone was not mine.'*

The individual was aware that beyond denial or forcibly creating some sort of destruction, they could not block authorities from accessing the device:

> *'There is no way to resist physically because you will be tortured until you open the phone.'*

For them, the most important issue was not further interrogation or the potential cost of blocking this access (they were arrested for political protests); the priority was to ensure that interrogators did not gain knowledge of their identity, which would put them at more mortal risk:

> *'The phone was not searched because I got rid of it … it contains an easy amount of information which could show that I am a queer person.'*

Others reported hiding their phones or using methods and tools to obfuscate or wipe the data from their phones (we have recommended this method before in the form of panic buttons[37]). One Sudanese interviewee outlined their second arrest:

> *'I was hit by whips, for my phone [but] I put my phone in the place where I was arrested before they took me to the vehicle.'*

In their first arrest, they used the features of their phone to wipe their phone and protect themselves (see below).

> *'Both times I was carrying my phone and both times I was able to protect my phone information, effectively.'*

Two of the Sudanese interviewees also arrested for their protest activities described hiding the phones on their person to avoid their device being found:

> *'The first thing I did when they arrested me immediately, I made my phone silent and tucked it into my bra. They put us in a minivan and let us sit in a squat position. The detention period was two days. … If they had obtained my phone, they might have identified my gender identity and my sexual orientation as well, but it wasn't used against me because I hid my phone.'*

Obfuscating data or no data in interrogations and searches

Some of the ingenuity shown in these cases revealed the resilience of the community in continuing to thrive despite threats and criminalisation. On top of the cases mentioned earlier, our interviewees spoke about the many methods they used to navigate and outsmart police, especially since they knew that their devices would be the 'scene of the crime' if captured.

In many of these cases people noted leaving their phones at home when summoned to the police station, which was especially the case in Egypt. For example, an interviewee in Egypt mentioned not using a smartphone at the time of arrest and thus having no

incriminating information on the phone he was carrying. Those arrested with him had smartphones on their person with their data accessible. Our interviewee was released; however, his friends received six-month sentences:

> *'I didn't have a modern phone with anything on it. Others did. They got six months. I was let go [because] they were not able to find any sort of information indicating that I was a member of the LGBTQI+ community on my electronic devices.'*

Importantly, this individual said he was wearing heteronormative clothing and could 'pass' as straight, which meant he was not profiled to the extent of his friends.

In another case where an Egyptian interviewee had been reported for making a social media post in remembrance of Sarah Hegazy, they had deleted their account and made a fake 'clean' account before being taken in for questioning – which of course required prior knowledge that they would be picked up:

> *'The two people stopped me and explained that they were from the police and asked me to accompany them to the police station in Qalyoub. … There they showed papers printed on them, the texts and pictures that I shared. [I] denied my connection to the account, and indeed when they opened it, they found it with a picture and a different name.'*

This individual was also very savvy, knowing that if they did not open their phone in the presence of the prosecution, the police could tamper with the evidence:

> *'They asked me to open my phone, and I refused to do that except in the presence of the prosecutor. They tried to threaten me, but I insisted on my position, and I was transferred to the prosecution the next day. I opened my phone in front of the prosecutor … and I opened a new Facebook account, and I denied my connection to the [previous] account. I was released from the Public Prosecution Office.'*

In Morocco, one of our sex worker interviewees outlined that it is common for queer sex workers to delete and obfuscate their apps, especially dating apps after departing for specific dates. This sex worker's informed savviness directly rescued them in at least one of their arrests:

> *'I had photos with make-up. But no nudes or photos with someone. … The good thing is I deleted Grindr. Because I usually disconnect and delete Grindr when I am with a certain type of client. And reconnect after.'*

Actively deleting apps or not having a phone on one's person was not always practical or doable – even for the most security-savvy of the community – as it was hard to predict when or where targeting and arrests could happen. As a result, many opted for more strategic harm reduction methods built into their devices. For example, one of our interviewees in Egypt used the safety features available on their apps to very successfully navigate device searches:

> *'I used the feature to change the icons of the dating application and change its name, so they could not find it, and I claimed that I forgot the password for social networking applications.'*

The feature used here is the **Discreet App Icon** feature on Grindr, which was introduced through our project's work with Grindr. The feature was based on our research on the habits and risks of technology applications in the policing of LGBTQI+ people. It is a great example of how combining methods used by the community to build features can be the difference between a prison sentence and release. In this instance, the use of this feature was the difference between receiving a sentence while under heavy interrogation and a release without charge. After claiming they had forgotten their passwords and refusing to provide passwords, the interviewee was still released because the officer failed to locate any incriminating data:

> *'The officer threatened to transfer me to the prosecution. I spent the night in the police station, but they released me the next day without referring me to the prosecution. … They were not able to find any sort of information indicating that I was a member of the LGBTQI+ community on my electronic [devices].'*

The combination of the two features was the saviour in this case. The interviewee suggested that if they could have obfuscated further without needing to plead that they did not remember the passwords, they could have also avoided that one day in detention.

Regardless, the outcome of this case is a great study for seeing safety features provided by apps in action.

Others report using tools to wipe the data from their phones (which has been recommended before as a panic button).[38] One Sudanese interviewee stated that they had successfully used features to wipe the data off their phone in one arrest and hidden their phone during another. During their first arrest they had managed to use a technological method that enabled their device's remote kill switch to block access to their content after it was confiscated – although this may not be an option for many arrestees. This meant that their data was secured on this occasion:

> *'The first time I was activating a feature called kill mode [switch], it hides the content of my phone and shows it as if the phone is empty.'*

On the second occasion, they did not take their device into the interrogation and hid the phone before arrest and interrogation:

> *'Both times I was carrying my phone and both times I was able to protect my phone information, effectively.'*

The Sudanese interviewee not only hid their phone but had also planned to use the features available to them on the device for securing the phone by making an invisible profile and using a safer interface (this is something that has been recommended before in the form of double PINs):[39]

> *'When I felt before the arrest that I was going to fall into their hands, I made my phone silent and hid it in my bra because this might be the last place they could be searched.*
>
> *Indeed, after the arrest and reservation, I completely denied that I had a phone.*
>
> *I also had an alternative plan which is an advantage in the iPhone and Android, which is the invisible profile as you change the profile and hide the other in order to keep the other secret as you know.*
>
> *I also made the option of covering the password.*

I had the phone with me, but I secured myself very well in the ways I mentioned above. But there is no information to indicate my orientation.'

Non-state outing, honey traps, violence, and extortion via apps

Some of the most reported abuses faced by the community were outings, doxxing, and extortion (sexual, financial, or other) through the use of people's devices and profiles. We often saw the worst types of abuses and financial and sexual extortion inflicted on members of the community with threats of outing and/or arrest.

Interviews:	**19 out of 93** (20%) interviewees had experienced **outings, doxxing,** and **extortion** (sexual, financial, or other) by non-state actors.
Surveys:	**291 out of 1,374** (21%) respondents mentioned being **robbed**. **189** (14%) mentioned **extortion**. Of these instances, more than 60% were linked to **app-based luring**. **181** (13%) mentioned **physical abuse**. **168** (12%) mentioned **entrapment** directly – predominately on dating apps such as SCRUFF, Grindr, Tinder, and Hornet, but also through social media such as Facebook, Instagram, Twitter, and others.

Some of the cases suggested that the groups or gangs that committed these crimes were doing so in collaboration with corrupt police. They often pretended to be police officers, regardless. One survey respondent said:

'In 2019, I met someone who came over to my place. I didn't notice that he kept the door open, so when we started to have sex, four police officers came and blackmailed me, and threatened to expose me to my family. They asked me to call my country's embassy because I'm a foreigner.'

Surveys:	**319 out of 1,374** (23%) respondents directly reported **extortion with threats of outing**: these were cases of overwhelming financial and sexual extortion. **43** respondents reported threats of **outing** and **defamation** that did not include a financial or physical element (often linked to revenge or bullying).

These cases highlighted the lack of protection and the societal risks of outing, and how this abuse of power has been so successfully used against members of the community.

Although it is not the focus of this report (which predominantly focuses on state-sponsored abuses and harm), here are some of the excerpts of **non-state outing and extortion** cases reported in our survey:

> *'I got blackmailed when I was 13 by a 19-year-old on Facebook Messenger. He used my nudes to blackmail me and, when refused, he shared them in a WhatsApp group with 30-year-old men from different ethnicities that later found my Facebook and harassed/blackmailed me. Some even found my school and neighbourhood. I stopped using socials for over two years because of that.'*

The rest of this testimony relating to the person's childhood experience shows the violence that ensued:

> *'I was stalked and almost raped by a 41-year-old who blackmailed me to go with him near a highway. Luckily I escaped. I couldn't sue him because I would have to tell my family, who would literally kill me instead of helping me.'*

Another young person explained that they had been outed by school peers who found information about their identity on Facebook. They bullied the individual, which eventually led to the respondent becoming homeless and nearly murdered.

In our interviews and focus group discussions, the issue of outing and extortion was also prominent, with **18 incidents reported**. The types of issue outlined included:

- Violence and outing after honey traps on dating apps.
- Outing of individuals based on digital profiles, either discovered or infiltrated – predominantly Facebook and Instagram.
- Outing on the discovery of profiles on a dating app – predominantly Tinder, Grindr, and Hornet.
- Outing based on access to dating apps and social media photos (even just profile photos used) – predominantly Facebook and Instagram combined with Tinder, Grindr, and Hornet.
- Hate speech and outings on YouTube.
- Reports and outings from private group chats on messenger apps.
- Screenshotting of conversations with numbers outed on WhatsApp stories.
- Outing and doxxing through mass forwarding on WhatsApp.
- Blackmailing especially of trans femmes.
- Stolen phones, with thieves using content for blackmail or outing.
- Extortion and threatening outing with videos and photos.
- Hacked phones leading to outing.

Our participants in all the research (interviews, surveys, and focus group discussions) described the **immense harm and abuse they faced after mass outing campaigns**.

One of the most prominent campaign was in Morocco in 2020. One interviewee in Morocco explained:

> *'The mass defamation campaign touched all the community in Morocco. It was a national event. All the people were targeting us.'*

This event was extensively documented by local groups and Human Rights Watch:

> *In Morocco, a campaign of outing emerged at the height of the Covid-19 pandemic in April 2020. People created fake accounts on same-sex dating applications and endangered users by circulating their private information on social media, including photos of men who used those applications, captioning the photos with insults and threats against the men based on their perceived sexual orientation. Because of this outing, many LGBT people were expelled from their homes during a country-wide lockdown and had nowhere to go. Moroccan LGBT activists informed Human Rights Watch about the outing phenomenon that caused panic among LGBT people who needed to protect their privacy due to social stigma towards homosexuality and the legal prohibition of same-sex relations.*

One of our survey respondents in Morocco mentioned the aftermath of this experience:

> *'In April 2020, some users pretended to be homosexuals for the sake of defaming the users of the app and exposing their information and photos on social media and Facebook groups. …. They were also expelled from their homes during quarantine. Some people committed suicide because they couldn't bear the humiliation of their families if they discovered their true identity.'*

This phenomenon was not new, and neither were its ramifications in Morocco (similarly elsewhere). In 2017, the Primary Court in Tangier sentenced two men to six months in prison for 'engaging in homosexual acts'. They were outed after a 90-second video of them circulated on WhatsApp.[40] Many other similar cases exist on platforms such as WhatsApp, Telegram, YouTube, Facebook, Instagram, and of course the dating apps, showing the prevalence and risks as well as the involvement of state abuses.

Our country expert in Algeria explained how this fear affects online expression:

> *There is the larger part of this population who have chosen to live in hiding and not reveal their identities. This [is because of the] daily fear of being unmasked [where they'll] suffer blackmail and harassment when malicious people discover their secret. Several documents published by the Algerian LGBTQI+ organisation TransHomosDz outline these abuses in universities, in companies, in family homes, and even in prisons.*[41]

In Jordan, our country expert team had similar comments:

> *Dating apps used by LGBTQI+ people have been exploited to blackmail and attack users. As a result of these issues, many LGBTQI+ people view online spaces as a minefield, instead of a safe haven. More recently, there have been cases of outing via social media channels, particularly a Facebook group that was created to gather members of the community in Jordan.*[42]

On 8 August 2014, an unidentified person published a blog post containing nearly 100 pictures of the Jordanian members of the Grindr and SCRUFF dating apps used by LGBTQI+ people.

Our country experts in Morocco summarised the reactions of the police after the mass outing campaign in Morocco. Shockingly, in light of the severe threats to people's lives, this demonstrated the pure **lack of impunity for these crimes**:

> *One of the victims was the young actor [name redacted] who was insulted by the influencer during a 'Live' on Instagram. [The influencer] encouraged her followers to rape the young man. He received many death threats. Following this situation, he tried to file a complaint for defamation, discrimination, and death threats. When he went to the police, the officer told him: "If you were my son, I would burn you alive", and accused him of non-compliance with confinement and contempt of public officials. They put him in police custody for 48 hours. [name redacted] got a suspended sentence of four months with a fine of 1,000 Moroccan dirham [USD 100]."*[43]

Prevalence of hate speech and the lack of support

Extensive work and documentation have been done showing the prevalence of hate speech on social media, dating apps, and chat-based apps that have very real-world impacts on people. Human Rights Watch recently launched a campaign with a focus on the failure of content moderation, especially on Meta platforms. In 2020, 22 LGBTQI+ organisations, mostly from MENA, urged platforms, especially Meta, to address the rising levels of hate speech on their platforms and address issues concerning the lack of

contextual, cultural, and linguistic understanding of their content moderators. Due to the immense amount of work done in this regard, our report only looks to echo the work of these campaigns, with some added data from our own research.

Note that this section does not contain data for Lebanon, but based on our work and the work of our partners in Lebanon, we know the findings here are also reflective of the situation in Lebanon.

Interviews:	**80 interviews** had a segment with a focus on hate speech. **70 out of 80** (88%) interviewees had directly experienced **hate speech online**. This was the most universal experience across all of our research countries. **41 out of 80** (51%) interviewees explained having no luck with their reporting, with the majority feeling platforms do not care about linguistically trained support for the region.
Surveys:	**235 out of 1,374** (17%) respondents who reported non-state-facilitated abuses in our surveys had experienced hate speech in the form of **harassment** (96 respondents), **threats** (127 respondents), and pure **homophobia** (12 respondents).

The concerning statistic here is the number of people (**41 interviewees**) who reported **little to no remedial action or content moderation support from the platforms**.

Some interviewees reported not only that the violent hate speech they had reported was **not acted upon** but also that they had received **responses that the content was not hate speech at all**. People reported experiencing transphobia, homophobia, racism, xenophobia, violent threats, doxxing, outing, revenge porn, and paedophilia, specifically.

Others mentioned specific features that allowed for cross-platform hate speech, outing, and harassment. For example, the feature on Tinder that allows users to share a link to a profile of an individual has been used to target queer-identifying people. Their profile was then shared across messaging platforms (this feature was said to be disabled as of the writing of this report). Others reported mass forwarding, as seen on

WhatsApp and other chat-based apps, as a major reason for massive hate speech and outing campaigns.

The following section delves deeper into the country-specific interviews.

Algeria

10 out of 10	Had experienced violent hate speech.
6 out of 10	Had had no luck/felt there was no moderation support.
5 out of 10	Mentioned Facebook not caring about Arabic and queer hate speech.

> *'I think that Facebook algorithms do not understand homophobic and misogynistic comments when they are in Algerian Arabic, so I think that Facebook must have algorithms or people working on these issues or they must analyse case by case to really understand the meanings of these comments.'*
>
> – Interviewee in Algeria

> *'Once I reported a Facebook account and it was not removed. Another time, I reported a user who asked me for paedophilic pictures and his account was never closed. Since then, I don't report anymore.'*
>
> – Interviewee in Algeria

> *'It appears that the people in charge of processing reports are not from the same background and it is difficult for them to really identify the reported hate speech.'*
>
> – Interviewee in Algeria

Egypt

10 out of 11	Had experienced violent hate speech.
4 out of 11	Had had no luck/felt there was no moderation support – and no longer report, especially trans interviewees.
8 out of 11	Mentioned Facebook not caring about Arabic for hate speech or queer content.

> *'Those who created the Arabic algorithms for these apps are privileged people, namely cis, hetero … men, who have normalised hate speech against people like us.'*
>
> – Egyptian focus group participant

> *'Tinder shouldn't let you share a link of other people's profiles which facilitates smear campaigns like the ones that happened in Maghreb and Egypt. There are even accounts dedicated to making fun of "weird Tinder profiles" on other social media apps.'*
>
> – Egyptian focus group participant

On 'shadow banning':

> *'If you're a queer individual sharing queer content, Facebook and TikTok usually block your content or make it less visible and lower the chances of it circulating. [Also] violators are left alone and queer [people] are banned instead.'*
>
> – Egyptian focus group participant

Iran

13 out of 14	Had experienced violent hate speech.
9 out of 14	Had had no luck/felt there was no moderation support – and no longer report, especially trans interviewees, and for Persian and queer content.
1 out of 14	Had been told on Instagram that violent hate speech was not against guidelines.

'In my opinion, the behaviour of companies is irresponsible in this regard. And this gives me the feeling of being ignored: "I'm dealing with this shit, but I'm absolutely alone in this and nobody is going to help me out."'

– Interviewee in Iran

'Algorithms do not recognise the Persian language. AI [artificial intelligence] is doing that job. In my opinion, content moderation should be the work of a person, not a robot.'

– Interviewee in Iran

Jordan

7 out of 10	Had experienced hate speech (especially homophobia combined with racism and sexism), including a YouTube influencer's doxxing of many people.
5 out of 10	Had had no luck in reporting/felt there was no moderation support in Arabic and queer context (including TikTok).
1 out of 10	Had been told on Instagram that violent hate speech was not against guidelines.

'As queers, we go to Facebook, we tell them there are people who want to burn us, who want to throw us off of buildings and they want to do this and that, and

Facebook doesn't take into account that this is hate speech and doesn't remove the comment.'

– Interviewee in Jordan

'Let's say they want to write [redacted Arabic slur] instead of writing it as it is, they would add a letter in the middle so the word won't look as it should be. A small change so the algorithm doesn't catch it but anyone that reads it knows what it is.'

– Interviewee in Jordan

Morocco

10 out of 10	Had experienced hate speech. The most mentioned app was Facebook and especially in Arabic.
5 out of 10	Had had no success in their reports and were told hate speech was not against policy. Reported having access to rapid responders who have privileged access to platforms to make reports, but even that did not work for them. Reported a lack of understanding context and slowness, even for death threats and massive violence.
1 out of 10	Mentioned no support for hate speech on dating apps.

'I once reported, and Facebook's response was that these attacks were not in opposition to their policies. Applications should be clearer and more precise about their rules regarding harassment and hateful and discriminatory speech.'

– Interviewee in Morocco

'I was a victim of hate speech on social media several times, especially after my outing. I received quite a few messages from people who threatened me with death. I reported it but without any result.'

– Interviewee in Morocco

Hate speech online had led to outing and physical violence against a trans woman interviewee in Morocco.

Sudan

12 out of 15	Had experienced hate speech, especially during the Fetrah campaign. Mostly on Twitter and Facebook.
7 out of 15	Had had no success in their reports directly and were infuriated. Reported having access to rapid responders who have privileged access to platforms to make reports, but even that did not work for them. Reported a lack of understanding context and slowness, even for death threats and massive violence.

'I reported it while working as a reference to Facebook in Sudan, but unfortunately, despite the strength of relations and communication, the result was always useless due to the company's policies. … Unfortunately, the policies and profits of companies stand in the way between what is demanded and what is happening.'

– Interviewee in Sudan

'The response will not be effective because their support teams may not know the context which will facilitate the spread of hate speech.'

– Interviewee in Sudan

'Hate speech on dating sites exists with accounts that are only created for that goal. My first account was on the Badoo app. I entered incorrect information about myself … the photo I had for the account was a flower. … Despite all of that, I received threatening messages and resentment. Twenty people reached out, 19 of them are threatening and calling me lesbian and a prostitute.'

– Interviewee in Sudan

Since the war started in April 2023:

> *'Hate speech has increased with the war, and the queer community was blamed as if they caused it due to their sins against God. I wish there was control over such speech.'*
>
> – Interviewee in Sudan

> *'A lot of videos documenting rape incidents were published. How was that allowed? Please implement the utmost surveillance on violent content and prevent its display.'*
>
> – Interviewee in Sudan

Tunisia

8 out of 10	Had experienced hate speech (especially homophobia combined with racism and sexism).
5 out of 10	Had had no luck in reporting/felt there was no moderation support in Arabic and queer context, including with NGO rapid responders.

> *'From the queer community … who faced problems on social media, there was nothing done to help them, or to protect them, or to make reporting easier for example.'*
>
> – Interviewee in Tunisia

> *'Put us in a category on our own because we need special attention, especially for the threats and problems we face online, which is not the same as other people, we are double threatened.'*
>
> – Interviewee in Tunisia

Impact of sanctions on the LGBTQI+ community: Iran and Sudan

Iran has been subject to sanctions since the inception of the Islamic Republic. As the grip of sanctions on the country has tightened over the past two decades, Iranians' access to various services, including communication and technology tools, has been increasingly disrupted. Despite efforts by civil society towards easing these disruptions, during the administration of the former US President Donald Trump and his 'maximum pressure' campaign against the Islamic Republic, several major technology companies started banning users based in Iran. The bans have adversely impacted Iranians' access to the internet and curtailed their freedom of expression, as detailed in ARTICLE 19's *Iran: Tightening the Net 2020* report.

Similarly, until recently, it was impossible to access any information and communication technologies and programs on the internet in Sudan because of the sanctions originally issued by the USA in 1997. This political and economic blockade impacted the ability of LGBTQI+ people in Sudan to access information on the internet or use technology to communicate securely. Sudan suffered an extended period of economic isolation following several sanctions imposed by the USA (and also the EU, UK, and UN) mostly due to the conflict in Darfur. The sanctions were gradually lifted, with the latest being the removal of the country from the US terrorism watchlist in 2020, leading to the commencement of some communications platforms' operations in Sudan. For example, Twitter started to allow Sudanese users to register accounts with a local phone number. Despite this, many app stores and communications and dating platforms have been slow to fully recommence operations in Sudan, adding to the isolation and internet blocks faced by the community. One Sudanese interviewee said:

> *'The idea of economic sanctions deprived us of specialised applications.'*

In Iran, these sentiments are felt even more deeply in a context where the population is suffering under one of the world's heaviest censorship and surveillance regimes.

7 out of 14 *(50%) interviewees in Iran directly mentioned feeling the impact of sanctions and finding the sanctions regimes discriminatory.*

5 out of 16 *(31%) interviewees in Sudan felt the impact of sanctions and the subsequent app blocks and felt they were discriminatory.*

This sentiment was felt towards dating applications that have blocked operations in both countries. These applications were seen as some of the only avenues people could connect via to find love and intimacy in these high-risk contexts.

Regarding the Grindr ban, one Iranian interviewee said that Grindr's decision to ban Iranians made him feel 'excluded and isolated'. He explained that the Islamic Republic had already blocked access to dating apps and many other communication and networking tools. According to him, the company's decision to ban Iranians made a bad situation worse. He said:

> *'These bans and limits are really awful. They have decreased my access to communication and networking tools. I knew some of the accounts on these apps were fake; however, when I had access to them, I had this hope that there's someone like me, someone living nearby that I could reach out to. Grindr's decision to ban Iranian users has killed that hope.'*

Others in Iran also felt anger towards platforms for too easily banning a population of people. As one Iranian interviewee put it:

> *'In my opinion, the fact that these applications arbitrarily block people's access without a valid reason plays a negative role against the queer community. Especially due to the role of these dating apps in closed societies like Iran, where people cannot contact each other in person.*
>
> *In practice, they are insulting Iranians. Maybe the reason is that they don't have any income from Iran because people can't buy premium services. That is yet another*

kind of discrimination. Because it means that basic services are free for everyone except Iranians.

With these restrictions that apps like Grindr have, the situation becomes even worse. It's like we have tripped and fallen already and then Grindr comes and kicks us too. OkCupid has also stopped its services in Iran. OKCupid does not allow you to join using a location in Iran. … It's as if they are pulling a dirty joke on us.'

As of the writing of this report, Grindr has recommenced its functionality in Iran as part of a collaboration effort with ARTICLE 19. Tinder, OkCupid, and many other dating apps remain inaccessible as far as our team is aware.

This idea that the bans have a direct impact on the queer community was a common sentiment. One interviewee said:

'This just puts pressure on Iran's gay community, not the government.'

This throttling has also meant limited access to what they deem as safer dating applications, including for hate speech. One Sudanese interviewee said:

'Hate speech is systematic, yes, but this situation differed with changing in the terms of privacy in some dating apps like … Harlem application, but unfortunately in Sudan it is not working because of the American sanctions.'

Another Sudanese interviewee hoped functionality could recommence so the queer community could safely message again:

'Dating sites are not working in Sudan because of American sanctions. But I hope that there will be specific messages for my country to the queer community in Sudan.'

Another said:

'Lift the restrictions on Tinder and allow it to work through local networks without the need for a VPN [virtual private network].'

An Iranian interviewee held this same sentiment regarding generalised dating applications like Tinder:

> *'Tinder does not allow Iranian numbers, they kicked us out. … This app was there for people, including queer people, to get to know each other. The fact that what they did affected Iranian users, and now we cannot use the app, means that they ignored our identity and experience as human beings.'*

This interviewee explained that the block has led to price gouging and off-market selling for phone numbers so people can still access these apps.

With country sanction bans, even with VPNs or other methods to circumvent sanctions, those in Iran and sometimes Sudan cannot receive SMS verification codes needed to sign up to most communication and dating platforms (see above).

Some respondents directly pointed to the human rights, discrimination, and racism issues related to these policies. An Iranian interviewee said:

> *'Companies like OkCupid do not provide service to users with Iranian IPs [internet protocols] or Iranian locations. This is an example of discrimination. There should be some kind of requirement for companies to serve everyone. Legally, it should not be possible for them not to serve a geographical area. … It makes no sense at all. It is officially a violation of human rights. An example of racism. You have stopped your services for a specific nationality. This is a violation of human rights.'*

The Sudanese queer community and the ongoing war

In April 2023, and in the midst of this research, a war broke out in Sudan between rival factions of the military government of Sudan: the Sudanese Armed Forces and the paramilitary Rapid Support Forces. As of April 2024, it has resulted in the killing of tens of thousands and the displacement of millions (see the Sudan section in Part I).

Our data gathering in Sudan had already been finalised by our Sudanese research team; however, we believed it was vital to try and gain some more current perspectives from the community while dealing with war and criminalisation in order to ensure our findings and

recommendations could better reflect their needs in this highly turbulent period. For this, Sam Adam, our Sudanese research lead, conducted five extra interviews – and also provided highly valuable insight for this period.

In our **post-war interviews**:

---

5 out of 5 *interviewees expressed needing financial support and safety online.*

5 out of 5 *interviewees mentioned intense isolation due to apps being blocked by censorship and sanctions.*

3 out of 5 *interviewees expressed that lack of internet access led to their further isolation and harm.*

1 out of 5 *interviewees saw an increased presence of security forces on dating apps.*

Our interviewees explained that they heavily relied on their digital communications to have access to their queer communities and to feel supported and safe, but due to the wartime situation, US sanctions, and widespread internet shutdowns in the country, they had lost this access. When the internet is available, it is very poor quality. As our country expert, Sam Adam, reported:

> *Banking applications were not working, and all the money was in these apps, making it hard to access the internet. Acquiring food and drink was very difficult; hence online presence was a secondary concern.*

WhatsApp was mentioned as an app that was heavily relied on for connection during the war; however, the interviewees felt WhatsApp was not invested in working to help these communities remain connected. They also mentioned that the safer dating apps that provided support and security features for them were blocked by sanctions, which harmed them in layered ways. Even for those using VPNs to access blocked or sanctioned apps,

the internet penetration levels were so low that they could not remain connected since VPNs often need stronger networks to provide this connection:

> *'I was also in contact with some people on Tinder, but due to poor network quality, I couldn't activate the VPN and, therefore, couldn't access and check on them.'*

One interviewee talked about Tinder and its lack of support and options – as well as the blocking of services in the country due to US sanctions. Others also cited a lack of access to free VPNs, generally.

Our country expert for Sudan explained the impact of this social isolation from the broader queer community in times of war:

> *Limited access to communication means – such as intermittent internet – severely hampers their ability to maintain these crucial connections. This forced isolation from one's support system during already trying times can magnify feelings of loneliness, exacerbating the mental and emotional toll of the conflict.*[44]

One interviewee expressed this isolation and its impact of not having access during this period:

> *'I feel separated. We've been displaced and now we are either refugees or internally displaced. There are no constant communication channels, and no platforms specifically for the queer community to identify needs or check on each other. As queers in Sudan, it takes a long time to form our trusted queer circles, and now we've been dispersed.'*

A similar sentiment was shared by another interviewee about the lack of access to their community:

> *'I desperately needed their presence at that time.*
>
> *After a long time, I found out that this close friend had lost his father in the war, and I wasn't there for him.'*

Another interviewee stated:

> *'In times of war, when we hear of an area getting bombed, I wanted to ensure my queer friends were safe, but I had to wait for hours for a network connection.'*

As our country expert for Sudan explained:

> *Based on the interview narratives, it is evident that the onset of war and the ensuing societal chaos only intensify familial pressures. The traditional family, already grappling with the strains of conflict, may become even less tolerant of a family member who identifies as queer. This internal conflict can manifest as emotional, psychological, and even physical violence."*[45]

For example, one interviewee explained:

> *'Outside, there are kidnappings, bombings, and random killings. Inside the home, it's the killing of my spirit.'*

This interviewee was outed during this period due to their family gaining access to their phone and they did not have a way to delete the data or block this access:

> *'When my family took my phone, I wasn't prepared for it. I didn't delete my private photos or messages, nor was I able to back up my data or log out of my emails. My life was exposed to them without any privacy.'*

On top of general access to online spaces and internet issues, there were risks of being looted, targeted, tortured, and aggressed by the militia and army forces. One of our interviewees, who was a trans woman, had experienced this targeting. She had lost all of her devices and access to the world while also being held captive:

> *'However, 20 days into the conflict, our house was raided by Rapid Support Forces soldiers. They robbed our home, harassed me and all of my sisters, stole all our devices, laptops, and phones. They held us captive in our home for two days, forcing the women among us to cook for them and wash their clothes. Since the moment they took my phone, I couldn't contact anyone until I found out that my other queer friends managed to escape.'*

Another interviewee had had a similar experience with the Rapid Support Forces when they took her devices and physically and sexually abused her:

> *'Physically, I was beaten and abused by members of the Rapid Support Forces. They sexually harassed me and threatened me with rape. They tried to unlock my phone and laptop, and when I refused to give them the passwords, they beat me severely.'*

She explained that women and femme people experienced much more violence:

> *'The violence I faced was because I'm a woman, which shows that even in times of conflict, women of all spectrums are the primary affected party.'*

Many Sudanese are queer refugees in host countries, which are now making them more vulnerable to xenophobia, abuse, lack of protection, and violence. Our country expert for Sudan explained:

> *Migration brings its own set of challenges, especially for queer individuals. Host communities, already strained by resource crunches, might not always be welcoming. Pre-existing biases against queer individuals can get intensified. The newcomers, instead of finding solace, might face ostracisation or even hostility, amplifying their vulnerabilities [which many Sudanese refugees have faced].'*[46]

One interviewee described the risks they faced when they passed checkpoints and borders:

> *'Also, when we were at checkpoints during travel, I was afraid that the soldiers would take my phone and harm me upon discovering my sexuality. The war came suddenly, and I was not prepared in terms of my safety and my data.'*

The situation in Sudan is very unpredictable and is '[one of the worst humanitarian nightmares in recent history]', according to Martin Griffiths, UN Under-Secretary-General for Humanitarian Affairs and Emergency Relief Coordinator. People, and especially the queer community of Sudan who are a pivotal part of Sudanese life, need more support, including safety and access in these times of unspeakable crisis.

Through discussions with our participants, our country expert for Sudan sees hope:

> *Sudan, in its current state of upheaval, unexpectedly presents a silver lining for marginalised communities. A queer activist rightly pointed out the unique advantage this unrest grants the queer community: 'In this pivotal moment for Sudan, every citizen faces the same threat, blurring our past divisions. It's imperative we seize this chance to regroup, remobilise, and reshape the queer movement.* ***Transcending our internal conflicts, we must unite under our shared goal: the safety and rights of the queer community. Now is our time, not just to survive, but to assert and thrive****."*[47]

Endnotes

[1] As well as from the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researcher Youba Darif on political, social, and legal issues of Morocco.

[2] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researcher Youba Darif on political, social, and legal issues of Morocco.

[3] Rigot, A. and ARTICLE 19 (2022) Digital Crime Scenes: The Role of Digital Evidence in the Persecution of LGBTQ People in Egypt, Lebanon, and Tunisia; see p. 121 on the prevalence of WhosHere for entrapments and their lack of safety measures.

[4] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team Bedayaa on political, social, and legal issues of Egypt.

[5] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team Bedayaa on political, social, and legal issues of Egypt. For more on this and the tactic of fabrication, see Rigot and ARTICLE 19, Digital Crime Scenes.

[6] Case file from the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team Bedayaa on political, social, and legal issues of Egypt.

[7] Rigot and ARTICLE 19, Digital Crime Scenes, p. 121 on the prevalence of WhosHere for entrapments and their lack of safety measures.

[8] Rigot and ARTICLE 19, Digital Crime Scenes.

[9] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local partner Mawjoudin on the social, political, and legal issues in Tunisia.

[10] United Nations Office on Drugs and Crime (2009) Physical and electronic surveillance; Rigot and ARTICLE 19, Digital Crime Scenes.

[11] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team Bedayaa on political, social, and legal issues of Egypt.

[12] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researcher Youba Darif on political, social, and legal issues of Morocco.

[13] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by Helem, Genwa Samhat, and legal experts in Lebanon on political, social, and legal issues of Lebanon.

[14] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by Helem and Genwa Samhat, and legal experts in Lebanon on political, social, and legal issues of Lebanon.

[15] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by Helem and Genwa Samhat, and legal experts in Lebanon on political, social, and legal issues of Lebanon. See also Human Rights Watch (2013) 'It's Part of the Job': Ill-treatment and Torture of Vulnerable Groups in Lebanese Police Stations, 26 June.

[16] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[17] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by Helem and Genwa Samhat, and legal experts in Lebanon on political, social, and legal issues of Lebanon.

[18] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[19] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[20] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[21] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[22] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team in Jordan on political, social, and legal issues of Jordan.

[23] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[24] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[25] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team in Jordan on political, social, and legal issues of Jordan.

[26] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local partner Mawjoudin on the social, political, and legal issues of Tunisia. A 'dead name' is the name a trans person was given at birth but no longer uses.

[27] Barman, A. (2022) Viceroy targets child safety, data protection of minors in second report on Truecaller, *Economic Times*, 29 September; Castro, C. (2022) Spammed if you do, spammed if you don't: is Truecaller putting your privacy at risk?, *Tech Radar*, 14 October.

[28] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[29] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[30] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by Helem, Genwa Samhat, and legal experts in Lebanon on political, social, and legal issues of Lebanon.

[31] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by Helem, Genwa Samhat, and legal experts in Lebanon on political, social, and legal issues of Lebanon.

[32] From the research briefing provided between 2022 and 2023 to ARTICLE 19 by Iran expert Khosro Isfahani on political, social, and legal issues of Iran.

[33] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researchers Azza Nubi and Sam Adam on political, social, and legal issues of Sudan.

[34] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local partner Mawjoudin on the social, political, and legal issues of Tunisia.

[35] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local partner Mawjoudin on the social, political, and legal issues of Tunisia.

[36] We analyse and outline the number of results based on how many people responded to a particular question or section and not the whole number of survey respondents. In this case, 5,018 people responded to this question.

[37] Rigot and ARTICLE 19, Digital Crime Scenes, p. 140.

[38] Rigot and ARTICLE 19, Digital Crime Scenes, p. 140.

[39] Rigot and ARTICLE 19, Digital Crime Scenes, p. 49.

[40] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researcher Youba Darif on political, social, and legal issues of Morocco.

[41] From the research briefing provided to ARTICLE 19 in 2022 by our local research team in Algeria on political, social, and legal issues of Algeria.

[42] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local research team in Jordan on political, social, and legal issues of Jordan.

[43] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researcher Youba Darif on political, social, and legal issues of Morocco.

[44] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researchers Azza Nubi and Sam Adam on political, social, and legal issues of Sudan.

[45] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researchers Azza Nubi and Sam Adam on political, social, and legal issues of Sudan.

[46] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researchers Azza Nubi and Sam Adam on political, social, and legal issues of Sudan.

[47] From the research briefing provided to ARTICLE 19 between 2021 and 2023 by our local researchers Azza Nubi and Sam Adam on political, social, and legal issues of Sudan.