PRIVACY INTERNATIONAL

Human Rights Committee 116th Session

The Right to Privacy in Morocco

Suggestions for right to privacy-related questions to be included in the list of issues on Morocco, Human Rights Committee, 116th Session

March 2016

Main concerns on the right to privacy and state surveillance in Morocco

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation. Any interference with the right to privacy can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human right.[1]

Privacy International has on-going concerns on the practices of unlawful surveillance by Moroccan law enforcement and intelligence agencies targeting independent journalists, human rights defenders and perceived opponents of the government. These practices occur in a context of ongoing, serious violations of the right to freedom of expression, association and peaceful assembly.

Article 24 of the 2011 Constitution of Morocco guarantees the right to privacy.

The Preamble of the 2011 Constitution of Morocco states that the Kingdom of Morocco commits itself to protect and promote the measures for human rights and international humanitarian law 'in their indivisibility and universality'. The Preamble also affirms that duly ratified international treaties have the primacy over the national law.[2] However, the Constitution expresses the supremacy of international treaties "within the framework of the dispositions of the Constitution and laws of the Kingdom, in respect of its immutable national identity (namely, Islam)".[3] This ambiguous wording renders the assertion of international treaties supremacy over national law unclear.

Lack of effective oversight of surveillance by law enforcement and intelligence agencies

There are at least eight government agencies that can potentially monitor communications. Under the authority of the Ministry of Interior, they include the "Renseignements généraux marocains" (also known as "Direction générale de sûreté nationale"), which is part of national police; and the "Direction générale de la surveillance du territoire" (DGST), dealing with counter-espionage and anti-terrorism and arguably the largest and most powerful agency. Under the authority of the Military, the "Direction générale des études et de la documentation" (DGED) and the "Service de Renseignement de la Gendarmerie Royale Marocaine".

1 Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also Report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org.

2 The Preamble of the 2011 Constitution of Morocco available at http://www.ancl-radc.org.za/sites/default/files/morocco_eng.pdf.

3 Ahmed Benchemsi, 'Morocco: Outfoxing the Opposition', 23 Journal of Democracy 57 (January 2012), p. 61, available at http://www.journalofdemocracy.org/sites/default/files/Benchemsi-23-1.pdf.

These services operate in near complete opacity. It is not known what legal provisions empower and regulate the activities of these agencies, nor what independent oversight mechanisms control their work.

Unlawful surveillance on journalists, political and social activists, human rights defenders

Violations of freedom of expression, association and peaceful assembly in Morocco has reportedly increased in recent years. Journalists, political activists, and human rights defenders have been unlawfully detained, prosecuted on politically motivated charges, tortured and ill-treated.[4]

Privacy International has documented how the Moroccan state security services have employed forms of unlawful surveillance to identify and target perceived opponents of the government.[5]

The systematic state surveillance by Moroccan security agencies has escalated since the Arab Spring and ramped up further since the February 20th Movement, - a series of protests took place in Morocco demanding democratic political and constitutional reforms around the time of the Arab Spring.[6] According to Amnesty International, police used excessive force against the protesters, activists affiliated with the movement were detained and some detainees were tortured and ill-treated in custody.[7]

Some of the surveillance in Morocco has been conducted by using sophisticated surveillance technologies (described below.) Other more traditional forms of surveillance and intrusion into people's privacy continue to be reported: neighbours and relatives of individuals perceived to be critical of the government have being visited by law enforcement agencies to obtain information or to intimidate them. Further, journalists and activists had their email and Facebook accounts hacked by groups of nationalist hackers perceived to be close to the government security agencies.[8]

Privacy is vital to support and reinforce freedom of expression. According to the UN Special Rapporteur on freedom of expression and opinion, "[S]tates cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications,

4 For more information on press freedom in Morocco see; Amnesty International, 'Amnesty International Annual Report 2014/2015 - Morocco/Western Sahara Report', (2014/2015), available at https://www.amnesty.org/en/countries/middle-east-and-north-africa/morocco/report-morocco/; Amnesty International, 'Morocco: Stop using 'terrorism' as a pretext to imprison journalists', (20 May 2014), available at https://www.amnesty.org/en/latest/news/2014/05/morocco-stop-using-terrorism-pretext-imprison-journalists/; Freedom House, 'Morocco: Freedom of the Press 2015', (2015), available at https://freedomhouse.org/report/freedom-press/2015/morocco.

5 Privacy International, 'Their Eyes on Me', (7 April 2015), available at https://www.privacyinternational.org/?q=node/554.

6 For more information on the February 20th Movement see; Human Rights Watch, 'Morocco: Thousands March for Reform', (20 February 2011), available at https://www.hrw.org/news/2011/02/20/morocco-thousands-march-reform; Amnesty International, 'Amnesty International Annual Report 2012 - Morocco/Western Sahara', (24 May 2012), available at http://www.refworld.org/docid/4fbe3923c.html; Freedom House, 'Freedom in the World 2012 – Morocco', (24 July 2012), available at http://www.refworld.org/docid/500fda38c.html.

7 Amnesty International, 'Morocco/Western Sahara: Two years too long - repression of protests must end', (20 February 2013), available at http://www.refworld.org/docid/5127354c2.html.

8 Privacy International, 'Their Eyes on Me', p. 9-11.

journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny".[9] Privacy International's investigation published in April 2015 on state surveillance in Morocco contains interviews with journalists and activists who have been personally targeted by state surveillance. Their testimonies show how state surveillance has been conducted to oppress journalists, political and social activists, and human rights defenders.

Hacking and other forms of surveillance technologies deployed in Morocco
The Moroccan government has invested significantly in the development of its capabilities to conduct communications and other forms of digital surveillance. According to documents leaked in July 2015 from the surveillance technology company Hacking Team, two Moroccan intelligence agencies have both purchased a highly invasive spyware surveillance technology, the 'Remote Control System' in 2009 and 2012.[10]

The spyware allows to: access any content stored on the computer; monitor in real time the use of the computer and what appears on the screen; log all the keys that are being hit, therefore giving away any passwords that are typed; capture screenshots; activate the computer's webcam and take pictures and videos.[11] The spyware costs an estimated €200,000. Hacking Team claims to sell solely to government and law enforcement clients.[12]

The UN Special Rapporteur on freedom of expression expressed his concerns over such offensive spyware and stated that "[F]rom a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter –inadvertently or purposefully- the information contained therein. This threatens not only the right to privacy and procedural fairness rights with respect to the use of such evidence in legal proceedings."[13]

Beyond the surveillance technologies marketed by Hacking Team, in 2011 the government reportedly invested €2 million in a surveillance system named Eagle (developed by Amesys Bull), that allows to perform censorship and mass monitoring of internet traffic, with a technique referred to as Deep Packet Inspection.[14]

In 2015, the Swiss government released a document that revealed the list of countries that bought surveillance technologies from Swiss companies.[15] Among the purchasers of advanced surveillance technology was Morocco that appeared to have tested mobile telecommunication interception or jamming equipment in 2013-14.[16]

9 Report by the UN Special Rapporteur on Freedom of Expression and Opinion, A/HRC/23/40, 17 April 2013, para. 79.
10 Privacy International, 'Facing the Truth: Hacking Team leak confirms Moroccan government use of spyware', (10 July 2015), available at https://www.privacyinternational.org/node/622.
11 Privacy International, 'Their Eyes on Me', p. 10. For a comprehensive report on the spyware and Hacking Team see Privacy International, 'Briefing for the Italian Government on Hacking Team's surveillance exports', (April 2015), available at https://privacyinternational.org/?q=node/561.
12 Privacy International, 'Their Eyes on Me', p. 10.
13 Report of UN Special Rapporteur on Freedom of Expression and Opinion, A/HRC/23/40, 17 April 2013, para. 62.
14 'Amesys: un Finger de Pop Corn pour le Croco', Reflets, (7 December 2011), (In French) available at http://reflets.info/amesys-un-finger-de-pop-corn-pour-le-croco/; 'Maroc : Le meilleur ami de la France se met au DPI grâce à Amesys, la filiale de Bull', Reflets, (30 November 2011), (In French) available at https://reflets.info/maroc-le-meilleur-ami-de-la-france-se-met-au-dpi-grace-a-amesys-la-filiale-de-bull/.
15 Privacy International, 'Swiss Government forced to reveal destinations, cost of surveillance exports', (14 January 2015), available at https://www.privacyinternational.org/?q=node/98.
16 'Bund lüftet Schleier um Big Brother', Tagblatt, (8 January 2015), (In German) available at http://www.tagblatt.ch/aktuell/schweiz/tb-in/Bund-lueftet-Schleier-um-Big-Brother;art120101,4089562.

It is notoriously difficult to identify who have been subjected to unlawful communications surveillance, particularly when employed by using malware. However, there are strong indications that the Remote Control System developed by Hacking Team was used to put activists under surveillance.

In 2012, research conducted by Citizen Lab, an interdisciplinary research group affiliated to the University of Toronto, identified the use of the Remote Control System against Mamfakinch.[17]

Mamfakinch is an online citizen media outlet that was founded in 2011 to cover and support the February 20th Movement. In 2012, all members of the editorial team of Mamfakinch received an e-mail that claimed to contain a document revealing a major scandal. In fact, the e-mail contained an offensive spyware, which, after running a forensic analysis of the spyware, Citizen Lab identified as being identical to a spyware technology 'Remote Control System'[18] designed and sold by Hacking Team.[19] Some members of Mamfakinch had been contributing anonymously and the malware could have been used to acquire information about their identities.

The chilling effect of this malware attack on the people contributing to Mamfakinch is hard to quantify. Since February 2014, Mamfakinch has been inactive. According to testimonies collected by Privacy International, the team is divided as to what led to the end of the publication. For some, it was a necessary break as the February 20th Movement it was originally meant to cover had ended. But for others, the team of Mamfakinch gradually left out of fear. The use of Hacking Team's spyware had suddenly raised the stakes: if the government was ready to invest so much money and efforts on putting them under surveillance, some felt that it was time to leave.

Recommendations

Based on the above observations, Privacy International proposes the following questions for the List of Issues:

Article 17

- What measures is Morocco taking to ensure that its state security and intelligence agencies respect the right to privacy in line with international human rights standards?

- In particular, how does Morocco ensure that all interception activities are only carried out in ways that comply with the principles of legality, proportionality and necessity?

- What are the mechanisms of oversight over the surveillance practices of Moroccan state security and intelligence agencies?

17 Privacy International, 'Their Eyes on Me', p. 18-19.
18 Ryan Gallagher, 'How Government-Grade Spy Tech Used a Fake Scandal to Dupe Journalists', Slate, 20 August 2012, available at http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html. See also; Privacy International, 'Their Eyes on Me', p. 18-19.
19 Privacy International, 'Their Eyes on Me', p. 18-19; For a more comprehensive overview of the issue see: 'Mapping Hacking Team's "Untraceable Spyware"', The Citizen Lab, 17 February 2014. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

- What type of surveillance technologies are employed by Moroccan law enforcement and intelligence agencies and how their use is regulated and monitored?

Article 19, 21 and 22

- What measures is Morocco taking to address the reports of unlawful surveillance of journalists, political activists and human rights defenders to ensure that their right to freedom of expression, peaceful assembly and association are respected and protected?