PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
27th Session – Kingdom of Morocco

The Right to Privacy in Kingdom of Morocco

Submitted by Privacy International

September 2016

Introduction

1. This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world.

2. PI wishes to bring concerns about the protection and promotion of the right to privacy in Morocco before the Human Rights Council for consideration in Morocco's upcoming review in 2017.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

4. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

Follow up to the previous UPR

5. There was no mention of the right to privacy within the context of communication surveillance and data protection in the National Report submitted by Morocco.[3]

6. A joint submission by Instance marocaine des droits humains (IMDH) and the Institute for Human Rights Studies (CIHRS) presented their concerns regarding the use of torture by the Directorate of Territorial Surveillance and domestic intelligence agencies[4] and Front Line Defenders reported that human rights defenders suffered intrusive surveillance.[5]

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil and Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; See also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

3 During the official review Sweden expressed its concern about recent measures to censor and restrict press freedom and to suppress freedom of expression via the Internet, but no recommendation was submitted. See: A/HRC/21/3, para. 30

4 See: A/HRC/WG.6/13/MAR/3, para. 37

5 Ibid, para. 72

Domestic laws related to privacy

7. Article 24 of the Moroccan constitution[6] contains a specific provision related to privacy:

> "Any person has the right to the protection of their private life.
> The domicile is inviolable. Searches may only intervene in the conditions and the forms provided by the law.
> Private communications, under whatever form that may be, are secret. Only justice can authorize, under the conditions and following the forms provided by the law, the access to their content, their total or partial divulgation or their summons [invocation] at the demand [charge] of whosoever..."[7]

International obligations

8. Morocco has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". The UN Human Rights Committee has noted that states party to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."

9. The Preamble of the 2011 Constitution affirms that duly ratified international treaties have the primacy over the national law. 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)".[8] This ambiguous wording renders the assertion of international treaties supremacy over national law unclear.[9]

Areas of concern

10. During the last decade, Morocco has achieved substantial progress with regards to its legislation on the protection of privacy. However, civil society organizations, independent media and international human rights organisations regularly point to the discrepancy between the law and its application and there have been numerous reports from journalists and human rights defenders of the on-going arbitrary and unlawful surveillance.[10]

6 Available at: http://www.maroc.ma/fr/system/files/documents_page/BO_5964BIS_Fr.pdf
7 General Comment No. 16 (1988), para. 1
8 Available at: http://www.maroc.ma/fr/system/files/documents_page/BO_5964BIS_Fr.pdf
9 Benchemsi, A., Morocco: Outfoxing the Opposition, 23 Journal of Democracy 57 (January 2012), p. 61.
10 Available at: http://www.journalofdemocracy.org/sites/default/files/Benchemsi-23-1.pdf
See: Privacy International, Suggestions for right to privacy-related questions to be included in the list of issues on Morocco, Human Rights Committee, 116th Session, March 2016. Available at: https://www.privacyinternational.org/sites/default/files/HRC_morocco.pdf;, Marquis-Boire, M., and Galperin, E., A brief history of governments hacking human rights organizations, Amnesty International , 11 January 2016. Available at: https://www.amnesty.org/en/latest/campaigns/2016/01/brief-history-of-government-hacking-human-rights-organizations/; Privacy international (2015), Their Eyes on Me – Stories of Surveillance in Morocco. Available at: https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

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

11. There are several government agencies that can potentially monitor communications but there limited publicly available information to be able to map out the entire law enforcement and intelligence apparatus of Morocco.

12. Under the authority of the Ministry of Interior, they include the Renseignements généraux marocains (RG), which is part of the Direction générale de la sûreté nationale (DGSN), the national police; the Direction générale de la surveillance du territoire (DST or DGST) dealing with counterespionage and anti-terrorism; the Service autonome de renseignement des Forces auxiliaires marocaines (FA); and the Direction générale des affaires intérieures (DGAI). In 2015, a counter-terrorism unit, the Central Bureau of Judicial Investigation (BCIJ), was founded and placed under the authority of the DGST.

13. Under the authority of the Military, the Conseil supérieur de la Défense nationale (CSDN), a council of Morocco's various security agencies; the Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), the Moroccan authority responsible for computer systems security and which supervises the work of the Moroccan Computer Emergency Response Team, known as ma-CERT; the Direction générale des études et de la documentation (DGED), the external spy agency; the 2e Bureau (2B), the military external spy agency, responsible for collecting external military intelligence; the 5e Bureau (5B), the military internal spy agency; and the Service de Renseignement de la Gendarmerie Royale.

14. With the King commanding the armed forces and intelligence services, and presiding over the judicial system, these services operate in near complete opacity. With the exception of the DST, which was put under partial judicial review since October 2011, it is not known what legal provisions empower and regulate most of the activities of these agencies, nor what independent oversight mechanisms control their work.

15. As early as 2005, the Head of the Equity and Reconciliation Commission (IER), a human rights and truth commission created[11] by King Mohammed VI to investigate past human rights abuses[12], lamented that he found it "difficult to obtain the regulations governing each of the various security agencies, their fields of action, their recruitment policies, their training, and methods of recruiting." "This lack of clarity," he warned at the time, "could make it easier for abuses to take place."[13]

11 United States Institute of Peace, Dahir approving Statutes of the Equity and Reconciliation Committee, Dahir No 1.04.42 of the 19th Safar 1425 (10 April 2004). Available at: http://www.usip.org/sites/default/files/file/resources/collections/commissions/Morocco-Charter.pdf

12 IER was criticized by parts of the human rights-community because it was not allowed to report about human rights violations occurring after 1999, when Mohammed VI was enthroned. IER was also attacked because it lacked the authority to publicly name perpetrators or to compel state agents to provide information.

13 Human Rights Watch, Morocco's Truth Commission: Honoring Past Victims during an Uncertain Present, November 2005, Volume 17, No. 11(e). Available at: https://www.hrw.org/sites/default/files/reports/morocco1105wcover.pdf

16. In its final report[14] addressed to king Mohammed VI in December 2005, IER called for[15]:

    - Developing and publishing the government's security policy;
    - Clarifying and publishing the legal framework regulating the institutional powers, the process of decision making, monitoring and evaluation mechanisms for all security agencies and administrative authorities;
    - Compelling the government to inform the public and parliament of any event requiring the intervention of security forces; and
    - Establishing internal control mechanisms within the security agencies, that are fair and transparent.

17. In December 2015, a national coalition of NGOs strongly criticized the persistent legal vacuum surrounding security and intelligence agencies. In a report submitted to the UN Human Rights Committee, they called on the government to comply with the requirements of international law, and in particular the ICCPR regarding the protection of privacy.[16]

18. International human rights standards require that intelligence agencies are subject to clear laws that appropriately delimit their powers; intelligence agencies should also be overseen by independent bodies to ensure they abide by domestic and international law.[17]

II. Expansive surveillance capabilities

19. The extent of the surveillance apparatus in Morocco remains unknown but evidence that has emerged over the last few years has indicated that the government has invested significantly in the development of its capabilities to conduct communications and other forms of digital surveillance.

20. 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.[18]

21. In 2015, the Swiss government released a document that revealed the list of countries that bought surveillance technologies from Swiss companies.[19] Among the purchasers of advanced surveillance technology was Morocco

14 Kingdom of Morocco, Justice and Reconciliation Commission, National Commission for truth justice and reconciliation, Summary of the Final Report, Dépôt légal: 2006/1780. Available at: http://www.cndh.org.ma/sites/default/files/documents/rapport_final_mar_eng-3.pdf

15 The Geneva Centre for the Democratic Control of Armed Forces (2009) La Réforme du Secteur de la Sécurité: À la lumière des recommandations de l'Instance Equité et Réconciliation du MarocEquité et Réconciliation du Maroc. Available at: http://www.dcaf.ch/Publications/La-Reforme-du-Secteur-de-la-Securite-A-la-lumiere-des-recommandations-de-l-Instance-Equite-et-Reconciliation-du-Maroc

16 Maroc: Rapport Alternatif de la Société Civile sur la Mise en Oeuvre du Pacte International Relatif aux Droits Civils et Politiques (PIDCP), Submitted by the Human Rights Committee in view of the UPR review of Morocco, 16 December 2015

17 See International Principles on the Application of Human Rights to Communications Surveillance

18 Reflets, Amesys: un Finger de Pop Corn pour le Croco, 7 December 2011. Available at: https://reflets.info/amesys-un-finger-de-pop-corn-pour-le-croco/; Reflets, Maroc : Le meilleur ami de la France se met au DPI grâce à Amesys, la filiale de Bull, 30 November 2011. Available at: https://reflets.info/maroc-le-meilleur-ami-de-la-france-se-met-au-dpi-grace-a-amesys-la-filiale-de-bull/

19 Page, K., Swiss Government forced to reveal destinations, cost of surveillance exports, Privacy International. Available at: https://www.privacyinternational.org/?q=node/98

that appeared to have tested mobile telecommunication interception or jamming equipment in 2013-14.[20]

22. According to documents leaked in July 2015 from the surveillance technology company Hacking Team, two Moroccan intelligence agencies purchased a highly invasive spyware surveillance technology, the 'Remote Control System'.[21] The CSDN and DST both purchased Remote Control System, Hacking Team's flagship spyware, using a company called Al Fahad Smart Systems, based in the United Arab Emirates, as a middleman. The CSDN first acquired it back in 2009 and the DST in 2012.[22] The spyware costs an estimated €200,000. Hacking Team claims to sell solely to government and law enforcement clients.[23]

23. The leaked documents showed the two intelligence agencies have been renewing their contracts with Hacking Team and, as of July 2015, were still reportedly using the spyware. Since 2009, according to the same documents, Morocco has spent well over €3 million on Hacking Team equipment.

24. Moreover, in April 2015, the Moroccan Royal Gendarmerie was listed as an "opportunity" for a €487,000 contract and said to be "very interested" in Hacking Team products, "especially for mobile", according to leaked internal documents.[24]

25. In 2013, the UN Special Rapporteur on freedom of expression expressed his concerns over such offensive spyware such as those marketed by Hacking Team.[25] The fact that Morocco has reportedly acquired this technologies is of particular concern, given the lack of publicly available laws and policies to regulate the activities of the intelligence agencies.

III. Unlawful surveillance of journalists, political and social activists, human rights defenders

26. In recent years, there have been increasing reports of journalists, political activists, and human rights defenders having been unlawfully subjected to surveillance, detained, prosecuted on politically motivated charges, tortured and ill-treated.[26]

20 Gafafer, T., Bund lüftet Schleier um Big Brother, Tagblatt, 8 January 2015. Available at: http://www.tagblatt.ch/nachrichten/schweiz/tb-in/Bund-lueftet-Schleier-um-Big-Brother;art120101,4089562

21 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.

22 Wikileaks, Hacking Team, 8 July 2015. Available at: https://wikileaks.org/hackingteam/emails/

23 Privacy international (2015), Their Eyes on Me – Stories of Surveillance in Morocco, pp. 10. Available at: https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

24 Wikileaks, Hacking Team, 8 July 2015, Available at: https://www.documentcloud.org/documents/2164669-royal-gendarmerie.html

25 "[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." See: Report of UN Special Rapporteur on Freedom of Expression and Opinion, A/HRC/23/40, 17 April 2013, para. 62

26 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 (2015) Morocco: Freedom of the Press 2015. Available at https://freedomhouse.org/report/freedom-press/2015/morocco

27. Some of the surveillance 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.[27]

28. 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.[28]

29. Privacy International's report 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, using hacking and other forms of surveillance technologies.[29]

30. 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 publishing collective Mamfakinch.[30]

31. 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'[31] designed and sold by Hacking Team.[32]

32. Some members of Mamfakinch had been contributing anonymously and the malware could have been used to acquire information about their identities.

27 Privacy international (2015), Their Eyes on Me – Stories of Surveillance in Morocco, pp. 9-11. Available at: https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

28 Report by the UN Special Rapporteur on Freedom of Expression and Opinion, A/HRC/23/40, 17 April 2013, para. 79

29 Privacy international (2015), Their Eyes on Me – Stories of Surveillance in Morocco, pp. 10. Available at: https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

30 Ibid, pp. 18-19.
Gallagher,R., How Government-Grade Spy Tech Used a Fake Scandal to Dupe Journalists, Slate, 20 August 2012.

31 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 (2015), Their Eyes on Me – Stories of Surveillance in Morocco, pp. 18-19. Available at: https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf

32 For a more comprehensive overview of the issue see: Marczak, B., Guarnieri, C., Marquis-Boire, M., and Scott-Railton, J.,Mapping Hacking Team's "Untraceable Spyware", The Citizen Lab, 17 February 2014. Available at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

The chilling effect of this malware attack on the people contributing to Mamfakinch is hard to quantify but since February 2014, Mamfakinch has been inactive.[33]

33. During the regional and local elections in September 2015, 30,000 mobile phone lines were reportedly tapped across the country. The mass surveillance operation was ordered by the Ministry of Interior which had set up commissions headed by Crown Prosecutors to supervise the operation. The authorities, who publicly admitted the operation, explained that the measure was dictated by "the desire to ensure a degree of transparency in the election."[34]

34. The list of individuals targeted by the operation included candidates, regional or provincial party officials, in addition to local government officials and people with no direct link to the vote but whose "occupations or activities" were deemed "related to the elections," according to the Ministry.

IV. Limitations on the use of encryption

35. Act 53-05 of 2007[35] on the electronic exchange of legal data restricts the use of encryption with "the import, export, supply, operation or use of means or cryptographic services" subject to a prior statement and prior approval from the government. Heavy penalties are reserved for the unauthorized use of encryption means.[36]

36. In January 2015, the government issued Decree 2-13-881[37] transferring the authority for the approval and monitoring of electronic certifications and regulation of encryption means from the Agence Nationale de Réglementation des Télécommunications (ANRT), a civilian agency, to the military (the General Directorate for the Security of Information Systems, or DGSSI) which became the national authority with the power to approve and monitor electronic certifications.

37. Moreover, the ambiguous legal framework fails to clearly outline whether the Act 53-05 also applies to the personal use of encryption. The lack of clarity is concerning and fails to provide users with a clear understanding on whether they may be prosecuted for using encryption tools.[38] This results in a chilling effect with citizens not trusting the internet as a safe space where they can speak freely and anonymously.[39]

33 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.

34 Le 360, [illegible] 30, 3 September 2015. Available at: http://ar.le360.ma/politique/60875

35 Act 53-05 of 2007, Available at: http://www.egov.ma/sites/default/files/files-wysiwyg/Loi%20n%C2%B053-05%20relative%20%C3%A0%20l'%C3%A9change%20%C3%A9lectronique%20de%20donn%C3%A9es%20juridiques.pdf

36 The unauthorised use of encryption without prior declaration or official approval is punished with one-year imprisonment and a fine of up to 100,000 dirhams (US$10,000). The court may also order the forfeiture of cryptographic means involved.

37 Bulletin officiel n° 6332 du 15 rabii II 1436 (5-2-2015), Available at: http://adala.justice.gov.ma/production/html/Fr/liens/..%5C188896.htm

38 Privacy International, Article 19 and International Human Rights Clinic at Harvard Law School (2014) Securing Safe Spaces: Encryption, online anonymity, and human rights. Available at: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf, pp. 14

39 Ibid, pp. 20-21

38. Human rights and pro-democracy activists have been worried that the vague language of the law could lead to encroachments on free speech and unfair prosecutions. In December 2015, a coalition of 14 local human rights NGOs condemned the restrictions imposed on the use of encryption calling for a complete decriminalization of its use.[40]

39. As the UN Special Rapporteur on Freedom of Expression has noted, "Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attack".[41]

V. Identification and registration of subscribers

40. Since April 2014, ANRT, the telecom regulator, has compelled mobile operators to identify their mobile subscribers, including prepaid SIM cardholders.[42] The ANRT justified the measure by the agency's efforts to comply with Act 09-08 on the protection of individuals with regard to the processing of personal data.

41. Compulsory SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups.[43] It can have discriminatory effect by excluding users from accessing mobile networks.

42. In 2015, the UN Special Rapporteur on freedom of expression recommended that "states should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users."[44]

VI. Crackdown on civil society

43. On two occasions, events organised by Privacy International with and by its local partners were shut down forcing the event being moved.[45] This is not a unique incident of abuse of human rights in Morocco, and wide-spread abuse has been documented and expressed by a variety of authoritative sources including Human Rights Watch[46], Amnesty International[47], and Reporters Without Borders[48].

40 Maroc: Rapport Alternatif de la Société Civile sur la Mise en Oeuvre du Pacte International Relatif aux Droits Civils et Politiques (PIDCP), Submitted by the Human Rights Committee in view of the UPR review of Morocco, 16 December 2015
41 A/HRC/29/32, para 16.
42 Agence Nationale de Réglementation des Télécommunications, Identification des abonnés mobiles: Les nouvelles mesures, Press release, 11 February 2014. Available at: https://www.anrt.ma/sites/default/files/CP-identification-abonnes-Fr.pdf
43 A/HRC/23/40, para 70; A/HRC/29/32, para 51
44 A/HRC/29/32, para 60
45 See: Drugeon, A., Le numérique, nouvelle frontière du combat pour les libertés, Telquel, 2 September 2014. Available at: http://telquel.ma/2014/09/02/numerique-combat-libertes_1414821; PanoraPost, L'association des droits numériques accuse, l'Intérieur interdit, el Khalfi dement, 8 May 2015. Available at: http://panorapost.com/article.php?id=10572
46 See: Human Rights Watch, Morocco/West Sahara. Available at: https://www.hrw.org/middle-east/n-africa/morocco/western-sahara
47 See: Amnesty Internationa, Morocco/West Sahara. Available at: https://www.amnesty.org/en/countries/middle-east-and-north-africa/morocco/
48 See: Reporters Without Borders, Morocco. Available at: https://rsf.org/en/morocco

44. In October 2015, seven activists and investigative journalists[49] were brought before the Tribunal of First Instance of Rabat and charged with 'using foreign funding to undermine State security', a charge that carries up to 5 years in jail.[50] The charges were widely seen as politically motivated.[51] These individuals were involved in a program funded by Dutch NGO Free Press Unlimited, to train journalists and human rights activists on reporting techniques as well as on tactics to evade government interception, including encryption.[52]

45. During their interrogation, the activists reported being shown transcripts of their private Skype and phone calls as well as copies of email exchanges. The defendants' lawyers also learned that at least one of the activists' phone was tapped for a period of three months.

46. The trial has been postponed three times already in the last year, and the next hearing has been schedule for 26 October 2016.[53]

VII. Shortcomings of data protection framework

47. In 2008 the adoption of Act N°09-08 established a framework for the protection of personal data and a data protection authority, la commission nationale de contrôle de la protection des données à caractère personnel (CNDP)[54].

48. The CNDP reports to the Prime Minister. It is responsible for advising the government and parliament on bills or legislative proposals and regulations related to the processing of personal data.

49. The CNDP does not exercise monitoring or regulation on the processing of data involving State security, defence, public safety or criminal offences. The limited powers of the CNDP is of concern, particularly in light of the Moroccan government's push towards national IDs and biometric databases.

50. In November 2013, the CNDP did publish a series of recommendations on the use of biometric devices, but focused exclusively on devices used for access control in a private setting.[55] The Commission is yet to look into the national IDs and biometric databases.

49 Free Press Unlimited, These seven Moroccan human rights defenders are on trial..., 18 November 2015. Available at: https://freepressunlimited.org/en/news/these-seven-moroccan-human-rights-defenders-are-on-trial

50 Human Rights Watch, Morocco: Drop Charges Against Activists Historian, Four Others Accused of 'Undermining Internal Security', 8 November 2015. Available at: https://www.hrw.org/news/2015/11/08/morocco-drop-charges-against-activists

51 Washington Post, Free speech goes on trial in Morocco, The Post's View, 20 November 2015. Available at: https://www.washingtonpost.com/opinions/free-speech-goes-on-trial-in-morocco/2015/11/20/9eaea2d2-8f9e-11e5-baf4-bdf37355da0c_story.html?utm_term=.b2c38f8cfb87

52 See: https://storymaker.cc/

53 Free Press Unlimited, Freedom of expression should not be on trial, 30 June 2016. Available at: https://www.freepressunlimited.org/en/news/freedom-of-expression-should-not-be-on-trial-0

54 See: http://www.cndp.ma/

55 CNDP, Délibération n° 478-2013 du 1er novembre 2013 portant sur les conditions nécessaires à l'utilisation des dispositifs biométriques pour le contrôle d'accès. Available at: http://www.cndp-maroc.org/images/deliberations/deliberation-n-478-2013-01-11-2013.pdf

Recommendations

51. We recommend that the government of Morocco to:

- Reform Morocco's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;

- Ensure that the relevant authority conducts an independent inquiry into the use of internet monitoring and intrusion software to assess their compliance with Morocco's domestic and international human rights obligations and make publicly available any findings related to the above inquiry;

- Halt all procurement of all surveillance technologies pending the results of the aforementioned requested inquiry and ensure there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses;

- Clarify the legal framework regulating encryption with regards to personal use of encryption;

- Abolish mandatory SIM card registration and review the data retention requirements placed on telecommunications companies;

- Investigate and act upon 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;

- Amend Act 09-08 to expand the role of CNDP from a regulator to a truly independent authority that is capable of holding private companies accountable and ensuring that the storage and processing of personal data carried out on behalf of the State and which involves State security and/or defence, does not indeed violate fundamental human rights;

- Enable the CNDP with a more forceful role in controlling the actions of the government and the private sector.