PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
27th Session – The Republic of Tunisia

The Right to Privacy in the Republic of Tunisia

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 Tunisia before the Human Rights Council for consideration in Tunisia's upcoming review.

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.

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 Tunisia. Despite being raised in the stakeholder report, the right to privacy and concerns for unlawful surveillance were not submitted in the recommendations.

6. The International Freedom of Expression Exchange Tunisia Monitoring Group (IFEXTMG) stressed the need for information to be revealed on the ramifications of the surveillance system established by the government of the former President Ben Ali and also reported first-hand reports that the Ministry of Interior was still tapping people's phones and emails.[2]

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 A/HRC/WG.6/13/TUN/3, para 53 and 54

Domestic laws related to privacy

7. The Constitution[3] of the Second Republic of Tunisia was adopted in January 2014 with a large majority. It came to life exactly two years after the ousting of former President Ben Ali. The new Constitution established human rights as a supreme guiding principle.

8. Article 24 consecrates the right to privacy, making the State responsible for:

> "... protect[ing] the privacy and inviolability of the home and confidentiality of correspondence, communications and personal data."

9. Article 32 guarantees the right of access to information:

> "The state guarantees the right to information and the right of access to information and communication networks."

10. Article 49 underlines the necessity and proportionality of limitations to those rights and highlights the discretionary role of the judiciary in any such limitations.[4]

11. Articles 128 establishes the Human Rights Commission which oversees respect for human rights and conducts investigations into their violation.

International obligations

12. Tunisia 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 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]."[5]

Areas of concern

13. Since the fall of the Ben Ali's government, there have been great advances to respect, promote and protection human rights in Tunisia. In particular, the adoption of a new Constitution on 27 January 2014 was a welcomed

3 Available at: http://www.legislation.tn/sites/default/files/news/constitution-b-a-t.pdf
4 "The limitations that can be imposed on the exercise of the rights and freedoms guaranteed in this Constitution will be established by law, without compromising their essence.
Any such limitations can only be put in place for reasons necessary to a civil and democratic state and with the aim of protecting the rights of others, or based on the requirements of public order, national defence, public health or public morals, and provided there is proportionality between these restrictions and the objective sought.
Judicial authorities ensure that rights and freedoms are protected from all violations.
No amendment may undermine the human rights and freedoms guaranteed in this Constitution."
5 General Comment No. 16 (1988), para. 1

advancement as it upheld Tunisia's commitment to fundamental rights and freedoms. However, the lack of transparency of the legacy of the Ben Ali's government particularly in terms of the on-going applicable laws and policies, and the practices of surveillance of citizens raises concerns and calls for the new government to provide more information on these issues. As Tunisia continues with its efforts towards political and legal reforms as a democratic state of government accountable to the rule of law, it is essential that issues related to privacy and data protection be addressed.

I. Communications surveillance[6]

14. During the government of President Zine El Abidine Ben Ali which was ousted in January 2011, there was widespread arbitrary surveillance of individuals as a means of exercising control, and repress legitimate political dissent.

15. Multiple examples of unlawful surveillance were reported. Bloggers and activists were arrested and detained and requested to disclose the passwords to their email and Facebook accounts.[7] Diplomatic cables from the US embassy in Tunisia released by WikiLeaks have also documented surveillance of activists who had been trying to reach out to foreign diplomats for help.[8]

16. As noted by the European Parliament, there are serious concerns that the surveillance infrastructure of the Ben Ali era are still in place in Tunisia.[9]

17. The 2014 Constitution guarantees fundamental rights and freedoms but there has been little reform yet to ensure that legislation comply with the new Constitution.[10]

Unaccountable new surveillance agency

18. The post-election government announced the creation of the Technical Agency for Telecommunications (ATT) through Decree No. 4506 of November 2013[11]. It operates under the supervision of the Ministry of Communication and Information Technologies, whose mission is to "provide technical support to the judicial investigations into the information systems of crimes and communication" as defined by Article 2 of the Decree.

6 Privacy International, State of Surveillance: Tunisia, February 2016. Available at: https://www.privacyinternational.org/node/743

7 See: Global Voices, Tunisia: blogger Fatma Riahi arrested and could face criminal libel charge, 6 November 2009. Available at: https://advox.globalvoices.org/2009/11/06/tunisia-blogger-fatma-riahi-arrested-and-could-face-criminal-libel-charge/ and Global Voices, Tunisia: Journalist and blogger Abdallah Zouari rearrested, 17 September 2009. Available at: https://advox.globalvoices.org/2009/09/17/tunisia-journalist-and-bloggger-abdallah-zouari-rearrested/

8 See: Wikileaks, Document available at: https://wikileaks.org/plusd/cables/06TUNIS2408_a.html; https://wikileaks.org/plusd/cables/09TUNIS791_a.html and https://wikileaks.org/plusd/cables/09TUNIS268_a.html

9 Directorate-General For External Policies Of The Union, After The Arab Spring: New Paths for Human Rights and The Internet in European Foreign Policy, Briefing Paper, Directorate B, Policy Department, EXPO/B/DROI/2011/28, July 2012. Available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT(2012)457102_EN.pdf, pp. 8-9

10 Human Rights Watch, Tunisia: Events of 2015. Available at: https://www.hrw.org/world-report/2016/country-chapters/tunisia

11 Decree No. 4506 of November 2013. Available at: http://www.legislation.tn/fr/detailtexte/D%C3%A9cret-num-2013-4506-du-06-11-2013-jort-2013-090__2013090045063?shorten=DBjx

19. The ATT was created to perform surveillance in accordance with investigative orders from the judiciary, therefore, only in the case of investigations launched by a court. The data collected would serve as evidence for prosecutors and presented to the court.

20. Despite the reassurance of the interim government the creation of the ATT raised concerns amongst human right groups who despite reassurances from interim governments feared that the policies and practices of Ben Ali would remain in place.[12]

21. The Decree No. 4506 raises concerns for its failure to uphold international human rights standards with regards to communications surveillance including[13]:

    - The ATT began to operate without any framework that defines the crimes they are mandated to investigate, since no law defines "crimes of information systems and communication" noted under Article 2 and does not refer to crimes defined in the Penal Code;

    - Article 9 refers to "office of legal proceedings that receives investigation orders", Article 11 to "investigations on orders received" and Article 6 "referral (of investigation orders) to the departments concerned with the obligation to specify reasons" but it fails to provide who issues these orders and what the procedures for request are;

    - Whilst the ATT was set-up to provide technical support to judicial investigations the agency itself is not subject to judicial control. As provided for by Article 1 the ATT is under the control of the Ministry of Information and Communications Technology and Article 12 provides for its Directors to be appointed by Decree by the same Ministry. These provisions completely side-line the Ministry of Justice;

    - Article 5 requires the ATT to undertake "any other mission linked to its activity that it is assigned by the ministry of information and communications technology" which raises concerns it may become a surveillance mechanism of the Ministry;

    - It does not provide for user notification prior, during or after they have been subject to surveillance by the ATT. This directly undermine an individual's ability to challenge the decision or seek other remedies.

    - It does not provide for a robust independent public oversight mechanism. Article 5 states that the annual reports of the agency would be 'secret, unpublished and only sent to the government.'

12 Abrougui, A. (2014) New Big Brother, non-existent reforms, in Global Information Society Watch 2014: Communications surveillance in the digital age, published by Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos). Available at: https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf, pp. 244

13 Reporters Without Borders, Authorities urged to rescind decree creating communications surveillance agency, 2 December 2013 and updated 20 January 2016. Available at: https://rsf.org/en/news/authorities-urged-rescind-decree-creating-communications-surveillance-agency

Furthermore, Section 2 of the decree established the creation of a committee to follow up on the work of implementation of the ATT but the mandate, operations and powers of this Committee were not defined and remain vague.[14]

- Article 16 exempts contracts linked to the operations of the ATT from being subject to transparency obligations which means the agency is subject to little scrutiny.

22. Furthermore, several restrictive laws continue to have effect even after the 2011 revolution and the "dismantling" of the police state of Ben Ali's government. Despite the creation of the ATT, it has been reported that the Ministry of Interior has continued to undertake communications surveillance of citizens, even if the number of these operations has decreased and are undertaken following receipt of written order from the State Prosecutor under the Code of Criminal Procedures which has yet to be reformed.[15]

Broad power to tackle terrorism

23. In the wake of the terrorist attacks which struck the Bardo Museum in Tunis on 28 March 2015, a new anti-terrorism law was sent to Parliament. It was adopted hastily without the required public consultation of relevant stakeholders such as the legal community, and civil society more broadly.[16]

24. The law adopted on 25 July 2015 by the Parliament, Law No. 26 on the Fight Against Terrorism replaced the 2003 counterterrorism law enacted by the Ben Ali administration.[17] The new law describes inter alia the legal framework for the interception and the monitoring of communications as part of a criminal investigations relating to a terrorist threat.

25. Lawful surveillance is put under the oversight and authority of the judicial power. It must be warranted by a judicial order issued by either an Investigative Judge or the Prosecutor of the Republic. The order must identify the specific types of communications subject to interception and/or monitoring, for a period that cannot exceed four months, and that can only be renewed once with a reason under Section 54(5). Data can be collected by the ATT, and from the servers of telecom operators and internet service providers. The law requires investigators to keep a written record of their surveillance operation at all times, and under Section 56(2) all of not leading to a criminal prosecution are protected by the data protection law.

14 Decree No. 2014-2891 of 30 July 2014. Available at: http://www.legislation.tn/fr/detailtexte/D%C3%A9cret-num-2014-2891-du-30-07-2014-jort-2014-065__2014065028913?shorten=iulc

15 Boumiza, K., Tunis : Les écoutes téléphoniques existent toujours, juste derrière le ministère de l'intérieur. 12 May 2013, African Manager, as quoted in Global Information Society Watch 2014: Communications surveillance in the digital age, pp. 245, published by Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos). Available at: https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf. Available at: www.africanmanager.com/150744.html

16 Le Courrier du Magrehb et de l'Orient, Tunisie – Pour votre sécurité…, September 2015. Available at: http://lecourrierdumaghrebetdelorient.info/tunisia/tunisie-pour-votre-securite/

17 Available at: http://www.legislation.tn/sites/default/files/news/ta2015261.pdf

26. Human rights and privacy advocates have, however, strongly denounced the vast powers the law has granted security forces. Amnesty International, Article 19, Avocats Sans Frontières – Belgique, REMDH, FIDH, Human Rights Watch, OMCT and the Carter Center publicly denounced the new law.[18] A number of provisions within the law have been identified as permitting abuse of the right to privacy and other fundamental rights as a result of their broad interpretations.[19] Concerns include:

    - A broad definition of terrorist offences "causing harm to private and public property, vital resources, infrastructures, means of transport and communication, IT systems or public services". This vagueness raises concerns of abuse which may permit the curtailment of fundamental rights and freedoms protected by international law including the right to protest;

    - The security and intelligence services are provided with extensive surveillance powers to use "special investigative techniques," which are not defined.

    - The power to decide to conduct surveillance is in the hands of the state prosecutor, who are still very much linked today to the executive, instead of independent judges;

    - Hacking being constituted as a crime of terrorist natures under Article 13(7) and the sanctions provide for 10 to 20 years of imprisonment and between Tunisian Dinars TDN 50.000-100.000;

    - The lack of protection for whistle-blowers who under Article 62 may be treated as criminals if they reveal information related to terrorist investigations and may face up to 10 years in jail;

    - The new law also sets up the National Commission to Fight Terrorism, an anti-terrorist standing committee tasked with leading the anti-terrorism effort but it side-lines the data protection authority, INPDP, which was not made party to the anti-terrorist standing committee;

    - Under Article 51, the Tribunal of first Instance is empowered to decide the take down and censorship of part or whole audio, videos and other digital publications which amount to terrorism or may be used to commit crimes;

18 Non-privacy related concerns include: the extension of custody from 6 to 15 days for suspects of terrorism, the authorisatin for hearing to take place behind closed doors with defendants unable to know the identity of the witneses and the re-introudction of the death penlaty for those judged guilty for an act of terrorism which led to a loss of lives. For more information see: Amnesty International, Tunisie : La loi antiterroriste met en péril les droits fondamentaux, 12 August 2015. Available at: http://www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/Tunisie-La-loi-antiterroriste-met-en-peril-les-droits-fondamentaux-15822

19 See: International Commission of Jurists, Tunisia: revise Counter-Terrorism Law to conform to international standards, 6 August 2015. Available at: http://www.icj.org/tunisia-revise-counter-terrorism-law-to-conform-to-international-standards/; Human Rights Watch, Tunisia: Counterterror Law Endangers Rights, 31 July 2015. Available at: https://www.hrw.org/news/2015/07/31/tunisia-counterterror-law-endangers-rights Amnesty International, Tunisie : La loi antiterroriste met en péril les droits fondamentaux, 12 August 2015. Available at: http://www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/Tunisie-La-loi-antiterroriste-met-en-peril-les-droits-fondamentaux-15822; Ben Youssef, D., Terrorisme et TIC : Carte blanche à Ammar404!, Nawaat, 25 August 2015. Available at: http://nawaat.org/portail/2015/08/25/terrorisme-et-tic-carte-blanche-a-ammar404/; Human Rights Watch, Tunisie: Des failles dans le nouveau projet de loi de lutte antiterroriste, 8 April 2015. Available at: https://www.hrw.org/fr/news/2015/04/08/tunisie-des-failles-dans-le-nouveau-projet-de-loi-de-lutte-antiterroriste

- Section 58 para 2 prohibits disclosure of identity of state agents undertaking hacking for any reason;

- Section 61 gives agents, after judicial authorisation, the power to enter private buildings or cars to implant surveillance devices outside the regular regulations of the criminal procedure code, ignoring time of day and target/property owner notification requirements in the code. Such orders can last two months and can be renewed once.

Surveillance capabilities

27. The extent of the surveillance apparatus in Tunisia, previously and currently, remains unknown but evidence that has emerged over the last few years have indicated President Ben Ali had purchased a wide range of surveillance technologies.[20] It remains unclear which technologies remain deployed and utilized by the new authorities.[21]

28. A former director of the ATI from 2008 to 2011 mentioned Trovicor GmbH (formerly a unit of Nokia SIemens Network) as one of the companies used for voice and data interception on cell phone. According to a report published by Bloomberg, the company is said to have provided Tunisia's phone companies with monitoring centres computers and also maintained their ability to feed calls and data to the listening posts, one of which included Ben Ali's presidential palace.

29. ETI A/S, a Danish company provided mobile data interception used to reconstruct online activities. This system is capable of tracking the websites a person visits and logs of e-mail correspondence. It is likely the product referred to is ETI's X-Stream which, according to a brochure, possesses that exact capability. Surveillance company Utimaco was reportedly hired to provide the infrastructure to relay the information the phone networks and the monitoring centres.[22]

30. In September 2013, Wikileaks published the "Spy Files", a trove of documents from 92 global intelligence contractors revealing that German company ATIS Huer sold a system named Klarios to Ben Ali's government.[23] The system "integrate[d] lawful interception and monitoring." It included "satellite monitoring, data retention and traffic monitoring."

20 Wagner, B., Exporting Censorship and Surveillance Technology, Humanist Institute for Co-operation with Developing Countries (Hivos), January 2012. Available at: https://www.hivos.org/sites/default/files/exporting_censorship_and_surveillance_technology_by_ben_wagner.pdf

21 Silver, V., Post-Revolt Tunisia Can Alter E-Mail With `Big Brother' Software, Bloomberg, 12 December 2011. Available at: http://www.bloomberg.com/news/articles/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software

22 Ibid

23 Wikileaks, Spy Files 3, 4 September 2013. Available at: https://wikileaks.org/spyfiles/docs/ATISUHER_ATISPres_en.html

Identification and registration of subscribers

31. Each mobile telephone user must present documentary evidence of his or her identity in order to purchase and activate a SIM card. SIM operators must record customer's identities, including name, surname, date of birth, address, and national identity numbers (CIN).

32. Under articles 8 and 9 of the Internet Regulations, ISPs are requested to record and submit lists of their subscribers to the authorities on a monthly basis and to retain content for up to one year.

33. In March 2014 in a bilateral meeting between the Ministry of Internal Affairs and the Ministry of Information and Communication Technologies, the ministries decided to revise the procedures for allocating SIM cards and strengthen requirements governing submission of supporting documents.[24] In July 2014, the telecommunications regulator sent an order requiring Orange Tunisia to respect the rules governing the sale of SIM cards and the conclusion of subscription contracts.[25]

Obligations imposed on internet service providers

34. In December 2014, Decree No. 2014-4773[26] was adopted to govern the liability of internet service providers (ISPs). It superseded the Decree No. 97-401 of 1997 and repealed the Regulations of 22 March 1997 which Article 8 required ISPs to submit a monthly list of subscribers to the authorities.

35. Whilst the new Decree is an improvement, it still imposes a duty on ISPs under Article 11 (3-4) to "to meet the requirements of the national defence, security and public safety in accordance with the legislation and regulation in force" and to "provide to the relevant authorities all the means necessary for the performance of his duties, in that context, the provider of Internet services shall respect the instructions of the legal, military and national security authorities".[27]

Limitations on encryption

36. The Telecommunications Code, first enacted in 2001, details, among other provisions, the conditions and procedures pertaining to the encryption of communications.[28]

24 See: Mosaique FM, 1 March 2014. Available at: http://archivev2.mosaiquefm.net/ar/index/a/ActuDetail/Element/36290-%d8%a7%d9%84%d8%af%d8%a7%d8%ae%d9%84%d9%8a%d8%a9-%d8%aa%d8%a8%d8%ad%d8%ab-%d9%81%d9%8a-%d8%a7%d9%85%d9%83%d8%a7%d9%86%d9%8a%d8%a9-%d9%85%d8%b1%d8%a7%d8%ac%d8%b9%d8%a9-%d8%a5%d8%ac%d8%b1%d8%a7%d8

25 Instance Nationale des Télécommunications, Press release, 24 July 2014. Available at: http://www.intt.tn/fr/index.php?typeactu=89&actu=508

26 Decree No. 2014-4773. Available at: http://www.legislation.tn/sites/default/files/fraction-journal-officiel/2015/2015G/007/Tg201447733.pdf

27 https://internetlegislationatlas.org/#/countries/Tunisia/frameworks/internet-regulation

28 Internet Legislation Atlas, Tunisia: Regulation of Internet intermediaries. Available at: http://www.legislation.tn/sites/default/files/codes/telecommunication.pdf

37. Under the Code, the unauthorized use of means or cryptography is punishable by up to 5 years in jail. Any use of such means requires a prior permission from the Agence Nationale de Certification (ANC).[29]

38. Many freedom of expression and privacy advocates have called for an amendment of the law in order to decriminalize the use of encryption.[30]

39. As the Special Rapporteur on Freedom of Expression has noted, "Outright prohibitions on the individual use of encryption technology disproportionately restrict freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression."[31]

II. Ineffective data protection framework

40. The National Authority for Personal Data Protection (INPDP)[32] was created in 2004 through Law No. 63 which established the personal data protection regime.[33] In 2007, Decree No. 2007-3003 defined its organization and functioning.[34]

41. The law requires private data controllers to apply for authorisation from the INPDP prior to the processing of personal data or for its transfer abroad.[35] The INPDP is also mandated to investigate privacy violations and to report to the government.

42. At a rare press conference in May 2016 in Tunis, the head of the INPDP listed some of the "most serious" violations that his institution has to deal with.[36] These included, among other violations, the unlawful harvesting of biometric data; the unlawful installation of surveillance cameras; the illegal use of personal data by telemarketers; the "wild transfers" of personal data abroad via offshore data servers; the unauthorized transfer of patients' medical data between healthcare providers.

43. Unlike the private sector, the government enjoys large exemptions with regards to the processing of personal data. The executive branch and the judicial power are granted vast discretionary powers in matters related to "national security", and in dealing with "sensitive data."

29 See: National Digital Certification Agency, Ministry of Communication Technologies and Digital Economy, Republic of Tunisia. Available at: http://www.certification.tn/

30 See: Human Rights Watch, Tunisia's Repressive Laws: The Reform Agenda, 16 December 2011. Available at: https://www.hrw.org/report/2011/12/16/tunisias-repressive-laws/reform-agenda; Article 19, Tunisia: Internat regulation, 4 April 2012. Available at: https://www.article19.org/resources.php/resource/3014/en/tunisia:-internet-regulation

31 Ibid, para 45.

32 See: National Authority for Personal Data Protection. Available at: http://www.inpdp.nat.tn/index.html

33 Organic Law No. 63 of 27 July 2004. Available at: http://www.inpdp.nat.tn/ressources/loi_2004.pdf

34 Decree No. 2007-3003 of 27 November 2007. Available at: http://www.inpdp.nat.tn/ressources/decret_3003.pdf

35 Ben Youssef, Protection de la vie privée en Tunisie : la loi et les modalités de son application, Nawaat, 30 October 2015. Available at: http://nawaat.org/portail/2015/10/30/protection-de-la-vie-privee-en-tunisie-la-loi-et-les-modalites-de-son-application/

36 Nawaat, INPDP : "La réalité de la protection des données personnelles en Tunisie et les défis à relever" …, 2 June 2016. Available at: https://nawaat.org/portail/2016/06/02/inpdp-la-realite-de-la-protection-des-donnees-personnelles-en-tunisie-et-les-defis-a-relever/

44. Privacy advocates have long called for a review of Law No. 63 to give the INPDP more independence from the executive branch and to expand its field of intervention so as to hold the government more accountable by giving it more independence and resources to undertake its mandate. And key concepts such as "sensitive data" should be better defined.[37]

45. The INPDP should also engage more actively with civil society and the media and help shift the current privacy vs. security debate from what the government sees as a zero-sum game, into an approach that favours achieving both privacy and security.[38]

Recommendations

46. We recommend that the government of Tunisia to:

- Take the necessary measures to review all laws that regulate surveillance or otherwise impact on the right to privacy of individuals to ensure they are compliant with international human rights law;
- Review the anti-terrorism law of 2015 and ensure its compliance with international human rights law, including the right to privacy;
- Undertake an investigation into the current surveillance infrastructure in Tunisia and dismantle all technologies that permit arbitrary mass surveillance of individuals;
- Review the Decree No. 5406 of 2013 to ensure that the ATT is subject to judicial control, independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;
- Abolish mandatory SIM card registration and review the data retention requirements placed on telecommunications companies;
- Amend the 2004 Personal Data Protection law to ensure that public institutions are subject to it;
- Ensure that the INPDP is appropriately resourced and independent, and has the power to investigate breaches of data protection principles and order redress.

37 Perarnaud, C., Data protection in Tunisia: a legal illusion?, iGmena. Available at: https://www.igmena.org/Data-protection-in-Tunisia-a-legal-illusion-

38 Ben Youssef, Protection de la vie privée en Tunisie : la loi et les modalités de son application, Nawaat, 30 October 2015. Available at: http://nawaat.org/portail/2015/10/30/protection-de-la-vie-privee-en-tunisie-la-loi-et-les-modalites-de-son-application/