Suggestions for privacy-related questions to be included in the list of issues on Tunisia, Human Rights Committee, 122nd session, March-April 2018

November 2017

Introduction

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. Tunisia signed the ICCPR status on the April 30th 1968, and ratified on Sep 23rd, 1988, along with accepting its optional protocol on June 29th, 2011[1].

Privacy International has on-going concerns on the practices of communications surveillance, registration obligations for mobile users, Internet Service Providers' obligations, restrictions on encryption, use of biometric and data protection framework in Tunisia.

The lack of transparency on 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 government to provide more information on these issues.

As Tunisia continues with its efforts towards political and legal reforms as a democratic state accountable to the rule of law, it is essential that issues related to privacy and data protection be addressed.

Tunisian Constitution guarantees on the right to privacy

The current Tunisian Constitution, adopted in January 2014, establishes human rights as a supreme guiding principle.

Article 24 enshrines 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."

[1] Ratification status of Tunisia. Available at: http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=178&Lang=EN

Article 32 guarantees the right of access to information in the following terms:

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

In regards with any limitations to these rights, Article 49 underlines the necessity and proportionality of them, and highlights the role of the judiciary in any such limitations:

- "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."

Finally, Article 128 establishes the Human Rights Commission which oversees respect for human rights and conducts investigations into alleged human rights violations.

Lack of accountability of surveillance agencies and powers

The extent of the surveillance apparatus in Tunisia, under the previous and current governments, remains unknown but evidence that has emerged over the last few years have indicated President Ben Ali had purchased a wide range of sophisticated surveillance technologies[2]. It is unclear which technologies remain deployed and used by the current authorities.

The Constitutional fundamental rights and freedoms have not yet fully reflected in ordinary laws.

The government elected following elections announced the creation of the Technical Agency for Telecommunications (ATT) through Decree No. 4506 of November 2013[3]. 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 is meant to be used as evidence for prosecutors and presented to the court.

[2] Wagner, Ben, 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

[3] Decree No. 4506 of November 2013. Available at: http://www.legislation.tn/sites/default/files/fraction-journal-officiel/2013/2013F/090/Tf201345063.pdf

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[4].

In particular, the Decree No. 4506 fails to uphold ICCPR standards in some of its provisions regarding communications surveillance, including the vagueness and broad nature of ATT's mandate (particularly in light of a catch-all provision contained in Article 5, requiring the ATT to undertake "any other mission linked to its activity"), the lack of judicial supervision of its activities, since the ATT is under the control of the Ministry of Information and Telecommunications Technology and its Directors are appointed by the same Ministry.

In the last review of Tunisia under the Universal Periodic Review process, Tunisia accepted the following recommendation submitted by Liechtenstein: "6.95. Bring all legislation concerning communication surveillance in line with international human rights standards and especially recommends that all communications surveillance requires a test of necessity and proportionality"[5]. Privacy International welcomes this and believes that the review by the Human Rights Committee offers an opportunity for the Tunisian government to show the concrete steps taken to review and reform its legislation and practice on this issue.

Overly broad counter-terrorism powers

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 without public consultations of relevant stakeholders such as the legal community.

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.

Human rights and privacy advocates have 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[6].

[4] 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), p.244. Available at: https://www.giswatch.org/sites/default/fles/gisw2014_communications_surveillance.pdf

[5] Section II of the Report of the Working Group 1/HRC/36/5 - adoption in plenary 21 September 2017

[6] Non-privacy related concerns include: the extension of custody from 6 to 15 days for suspects of terrorism, the authorisation for hearing to take place behind closed doors with defendants unable to know the identity of the witnesses and the re-introduction of the death penalty for those judged guilty for an act of terrorism which led to a loss of lives. For more information see: www.amnesty.fr/Nos-campagnes/Liberte-expression/Actualites/Tunisie-La-loi-antiterroriste-met-en-peril-les-droits-fondamentaux-15822See:

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 scope. Concerns include, among others:

- 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 peaceful assembly;
- 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.

Obligations imposed on mobile users and Internet Service Providers

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 (CCIN).

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.

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.

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.

In regards with Internet Service Providers (ISP), In December 2014, Decree No. 2014-4773 was adopted to impose liability to Internet Service Providers, superseding a Decree and Regulations from 1997, which contained provisions demanding ISP's to submit a monthly list of subscribers to the authorities.

Whilst the new Decree is an improvement, it still imposes a very vague duty on ISPs 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".

Both mandatory SIM card registration and the obligations to provide identity of subscribers to authorities significantly interfere with the right to privacy and limit the possibility of communicating anonymously, thereby limiting the right to freedom of expression. SIM card registration,, in particular,, violates privacy in that it
limits the ability of citizens to communicate anonymously. It also facilitates

the tracking and monitoring of all users by law enforcement and intelligence agencies. Research shows that SIM card registration is not a useful measure to combat criminal activity,, but actually fuels the growth of identity-related crime and black markets to those wishing to remain anonymous.[7]

Limitations on encryption

The Telecommunications Code, first enacted in 2001, details, among other provisions, the conditions and procedures pertaining to the encryption of communications[8]. 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 (AANC)[9].

Many freedom of expression and privacy advocates have called for an amendment of the law in order to decriminalize the use of encryption[10].

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"[11].

National biometric ID system

In December 2014, the Tunisian government revealed that the country was set to launch an electronic ID card and biometric passports by the end of 2016[12]. The new biometric documents (containing each a photograph and scanned fingerprints) will gradually replace the current identity papers. A bill entered the Tunisian parliament on the 5th of August of 2016, and it is under review in a parliamentary commission since the 19th of May of 2017[13].

---

[7] KP Donovan and AK Martin "The rise of African SIM registration: Mobility, identity, surveillance and resistance", Information Systems and Innovation Group Working Paper No. 186, London School of Economics and Political Science, London.

[8] Telecommunications code available at https://internetlegislationatlas.org/#/countries/Tunisia/laws/72

[9] See: National Digital Certification Agency, Ministry of Communication Technologies and Digital Economy, Republic of Tunisia. Available at: http://wwww.ccertifcation.tn/

[10] See: Human Rights Watch, Tunisia's Repressive Laws: The Reform Agenda, 16 December 2011. Available at: https://www.hrw.org/sites/default/files/reports/tunisia1111webwcover.pdf; Article 19, Tunisia: Internet regulation, 4 April 2012. Available at: https://www.article19.org/resources.php/resource/3014/en/tunisia:-internet-regulationIbid

[11] Report on of the UN Special rapporteur on freedom of expression, UN doc. A/HRC?29/32, 22 May 2015. Available at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[12] La Tunisie va passer à la carte d'identité électronique et au passeport biométrique. Available at: http://www.jawharafm.net/fr/article/la-tunisie-va-passer-a-la-carte-d-identite-electronique-et-au-passeport-biometrique/90/18365

[13] Projet de loi organique N°62/2016 amendant et complétant la loi N°27/1993 du 22 Mars 1993 relative à la carte d'identité Nationale. Available at: https://majles.marsad.tn/2014/fr/lois/57ce8ac9cf44123b7174acee

Recently, the African Development Bank approved a €71 million loan to strengthen Tunisia's public services through digitalisation, including "a digital ID system"[14].

The adoption of biometric ID systems carries several risks in relation with the creation of new databases and the potential of data breaches or facilitating surveillance activities. This is particularly so in light of the inadequacy of the current data protection laws in Tunisia (noted below.)

Ineffective data protection framework

The National Authority for Personal Data Protection (IINPDP) was created in 2004 through Law No. 63[15], which established a personal data protection regime. In 2007, Decree No. 3003 defined its organization and functioning[16]. 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[17].

The INPDP is also mandated to investigate privacy violations and report them to the government. It can also bring violators before the courts. In May 2016 in Tunis, the head of the INPDP listed some of the "most serious" violations that his institution has confronted[18]. They 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 through offshore data servers; and the unauthorized transfer of patients' medical data between healthcare providers.

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

[14] AfDB approves €71.56m loan to Tunisia for digitalisation. Available at: http://www.publicfinanceinternational.org/news/2017/11/adb-approves-eu7156m-loan-tunisia-digitalisation

[15] Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel. Available at: http://www.inpdp.nat.tn/ressources/loi_2004.pdf

[16] Décret n° 2007-3003 du 27 novembre 2007, fixant les modalités de fonctionnement de l'instance nationale de protection des données à caractère personne. Available at: http://www.inpdp.nat.tn/ressources/decret_3003.pdf

[17] Protection de la vie privée en Tunisie : la loi et les modalités de son application. Available at: https://nawaat.org/portail/2015/10/30/protection-de-la-vie-privee-en-tunisie-la-loi-et-les-modalites-de-son-application/

[18] INPDP : "La réalité de la protection des données personnelles en Tunisie et les défis à relever". 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/

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, but reform attempts have been stalling so far[19].

On November 1st, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention No. 108) entered into force in Tunisia[20], representing an opportunity for the country to move forward with a long overdue reform of their data protection law.

Recommendations

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

Article 17

- What measures does Tunisia intend to adopt in order to bring its legislation concerning communication surveillance in line with international human rights standards and complying with the necessity and proportionality tests?
- How does Tunisia ensure that the ATT and other surveillance agencies are receiving enough independent oversight from independent mechanisms?
- What type of surveillance technologies are employed by Tunisian law enforcement and intelligence agencies and how their use is regulated and monitored?
- How will Tunisia ensure that their initiatives on implementing new identification and/or biometric technologies will respect the right to privacy?
- What measures is Tunisia adopting to lift the current restrictions on the use of encryption?
- How does Tunisia ensure that the registration obligations imposed on mobile users and Internet Service Providers complies with the principles of legality, proportionality and necessity?
- What measures is Tunisia taking to reform its Data Protection Law and revise the overbroad exemptions granted to the government and the enforcement mechanisms of the Law, so it can improve its compliance with Convention No.108 and fall in line with international and human rights standards?

[19] Data protection in Tunisia: a legal illusion? Available at: https://cihr.eu/policy-analysis-data-protection-in-tunisia-a-legal-illusion/

[20] Chart of signatures and ratifications of Treaty 108. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=W4kPedSQ