The Right to Privacy in Senegal

Stakeholder Report
Universal Periodic Review
17th Session - Senegal

Submitted by Privacy International, and Jonction Senegal
March 2013

Introduction

This stakeholder is a submission by Privacy International (PI) and Jonction Senegal. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. Jonction Senegal is a human rights organisation based in Dakar, which aims to promote sustainable and equitable development and human rights both in Africa in general and in Senegal in particular. Together PI and Jonction Senegal wish to bring concerns about the protection and promotion of the right to privacy in Senegal before the Human Rights Council for consideration in Senegal's upcoming review.

The right to privacy

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. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, ad "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[2] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[3]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate a number of State obligations related to the protection of personal data.[4] A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law. Data protection is also emerging as a distinct human or fundamental right: numerous countries in Latin America and Europe have now recognised data protection as a

[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] 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] 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.

[4] 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).

[5] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

constitutional right, and the recently adopted ASEAN Human Rights Declaration explicitly applies the right to privacy to personal data (Article 21).

Follow up to the previous UPR

Senegal adopted its new data protection law, Law No 2008-12 on the Protection of Personal Data (discussed below), on 15th January 2008, approximately a year before the previous UPR, which took place on 6th February 2009. No mention was made of this law or of privacy in the context of data protection in general in the Working Group report.

International obligations related to privacy

Article 79 of the **Constitution of Senegal**[6] states that international law takes precedence over domestic law. Consequently, international human rights instruments are part of the domestic law of Senegal and take precedence over any discriminatory state law.

Senegal has signed and ratified the Universal Declaration of Human Rights ('UDHR') and the International Covenant on Civil and Political Rights ('ICCPR'), meaning that the Article 12 UDHR and Article 17 ICCPR, which provide for the right to freedom from arbitrary interference with privacy, family, home and correspondence, are part of Senegal's domestic law.

Domestic laws and regulations related to privacy

Article 13 of the **Constitution of Senegal** protects privacy of communications, stating:

'The secrecy of correspondence, postal, telegraphic, telephonic and electronic equipment is inviolable. No restriction on this inviolability is permitted except by operation of law.'[7]

Article 7 of the **Constitution of Senegal** guarantees all citizens 'basic freedoms, economic and social rights and collective rights', including 'civil liberties', although it makes no explicit mention of the right to privacy.[8]

Senegal adopted **Law No 2008-12 on the Protection of Personal Data**[9] on 15th January 2008. This is a broad and comprehensive data protection law, covering the collection, handling, transmission, storage and use of personal data by individuals, government entities, local authorities and legal persons operating under public or private law. The law applies to all processing of data on Senegalese territory and in any place where Senegalese law applies. The law does not apply to individuals processing personal data in their personal capacity, on condition that the data is not intended for systematic communication or dissemination to third parties.

[6] The Constitution is available at: http://www.gouv.sn/IMG/pdf/Constitution.pdf
[7] *Ibid.*
[8] *Ibid.*
[9] The Law is available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=181186

The law designates a Personal Data Protection Commission (CDP), whose role it is to ensure that any processing of personal data is in accordance with the law. Its responsibilities also include informing data controllers and data subjects of their rights and obligations, handling complaints, conducting audits, and sanctioning data controllers who are in breach of the law.

Article 20 outlines the types of personal data which require authorisation of the CDP before they can be processed. This includes genetic data and data concerning health research, personal data concerning offences, personal biometric data, national identification numbers, and historical, statistical or scientific data of notable public interest. When seeking authorisation, the data controller must provide detailed information, including his identity and address, the purpose for which the data is being requested, the duration of time for which the data will be held, those who will have access to the data, arrangements to ensure the security of the data, intended transfers of the data to other countries.

The law incorporates data protection principles from "International Standards on Data Protection and Privacy", including principles of legitimacy, consent, quality, purpose, proportionality and accountability. In sum, these principles ensure that data will be treated for the purposes intended, with full knowledge of the data subjects. The law also provides additional protections for sensitive personal data, which is defined in Article 40 as data concerning racial, ethnic or regional background, family relations, political opinions, religious and philosophical beliefs, trade union membership, sexuality, genetic data or data that generally concerns the individual's health. The processing of such data is prohibited, with certain exceptions, such as where the data is manifestly made public by the data subject or where he has given his consent.

Senegal incorporated **Law No 2008-11 on Cybercrime**[10] into its Penal Code on 25th January 2008. The law outlines penalties for the commission of various cybercrimes, including fraudulently accessing, maintaining presence in, obstructing and/or distorting the operation of computer systems, and inputting, intercepting and/or deleting data from computer systems. The penalties range from a prison sentence of six months to five years and/or fines from one million to ten million francs. The law also establishes penalties of one to seven years in prison and/or a fine of 500,000 to ten million francs for breach, even through negligence, of the personal data protection law.

Senegal also adopted **Law No. 2008-08 on Electronic Transactions**[11] on 25th January 2008. This law is intended to ensure the security of electronic transactions in Senegal, including transactions related to electronic commerce. It covers definitions of electronic transactions and electronic commerce, the transmission of electronic documents and administrative acts, agreement and conclusion regarding electronic contracts, and the acceptance of electronic signatures.

Areas of Concern

1. <u>Absence of independent data protection authority oversight</u>

[10] The Law is available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=243067
[11] The Law is available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=236001

We welcome the official establishment in February 2012 of this national data protection authority (the CPDP, or *Commission de Protection des Données Personnelles*). However, we have observed that its activities are effectively frozen, primarily because it has not been allocated an operational budget by the state. This is despite the fact that the functioning of this commission is essential to data protection oversight and the enforcement of Law No. 2008-12. This state of affairs hampers attempts to reinforce privacy protections in Senegal.

2. Registration of mobile telephony users

The director of Senegal's telecommunications regulator, the *Agence de Régulation des Télécommunications et des Postes* (ARTP), in decision 2006 - 001 ART/DG/DRJ/DT/D.Rég of 5th December 2006[12], obliges mobile telecommunications operators to identify their clients at the time of subscription and ensure that their corporate distributors proceed to identify clients before selling them Subscriber Identity Module (SIM) cards. This policy is justified using a public safety rationale, with the 2006 decision referring to potential disruptions to "public safety and tranquillity". This decision does not make reference to the rights of users to access their data or to rectify mistakes within this data. Operators do not have an obligation to inform users about the way in which their data is used and there is no stipulation for deletion of the data once the commercial relationship between user and operator is terminated.

We have been unable to receive responses to questions about SIM registration from the director of the ARTP (the telecoms regulator). Although the SIM registration law may be intended to assure public safety, the law must also take into account the rights of mobile telephony subscribers to their personal data. SIM registration undermines the ability of users to communicate anonymous and disproportionately disadvantages the most marginalised groups. It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilities surveillance and makes tracking and monitoring of users easier for law enforcement authorities.

We have noticed that SIM registration is sporadic in practice and SIM cards can easily be obtained on the street without registration required by the eventual user. This lack of enforcement notwithstanding, the relevant authorities should take privacy and data protection into account when enforcing the law.

3. Tracking of entry and exit at Dakar airport

Passengers arriving at and departing from Léopold Sédar Senghor (LSS) airport in Dakar are required to fill out landing and departure cards. On these cards, passengers passing through the airport must provide personal data in the relevant fields of the card (name, flight information, place of permanent residence, and more). This information is eventually transmitted to the Senegalese police, who are in charge of regulating flows at the country's official entry points. Once these forms are submitted, passengers have no access to their data or even any indication of how their data will be stored or transmitted.

Further to the completion of these landing cards, passengers are also subject to the collection of their biometric data: during the course of entry and exit passport control, passengers have the

[12] Law is available at: http://www.osiris.sn/Decision-no-2006-001-ART-DG-DRJ-DT.html

imprint of their index finger taken electronically. This biometric registration is run by a private corporation, Securiport LLC, which specialises in the production, running and maintenance of airport security and surveillance systems. Given that Senegalese and other nationals are thus having their data managed by a US-owned private company, we regard it as being especially important that the existing laws regarding the protection of personal data are applied and respected.

4. Communications monitoring

The United States State Department reports that illegal telephone monitoring by security services is common practice in Senegal.[13] If such reports are verified, this would constitute a violation of international standards regarding privacy of communications, and breach of Article 13 of the Senegalese Constitution.

Areas of Improvement

The introduction of **Law No 2008-12 on the Protection of Personal Data**, discussed above, is a welcome additional protection of privacy in Senegal. It is a significant and comprehensive piece of legislation which provides adequate safeguards to citizens' personal data. The law reflects the *habeas data* concept: the individual whom the personal data concerns is designated the "data owner" and is in possession of all relevant legal rights relating to use of that data. The law also effectively addresses the various and important factors relating to data protection, including notice, purpose, consent, security, disclosure, access, and accountability. As noted above, the law also incorporates principles from the "International Standards on Data Protection and Privacy", including principles of legitimacy, consent, quality, purpose, proportionality and accountability, as well as providing additional protection to sensitive personal data. Importantly, it establishes a commission, made up of eleven members appointed by the president and including judges, parliament deputes and officials of several government agencies, for watching over compliance with the law; this commission is accountable and has extensive powers, including the power to adequately sanction data controllers acting in breach of the law. This data protection law is particularly welcome in light of the ever-expanding use of the internet in Senegalese society.

The introduction of **Law No 2008-11 on Cybercrime**, discussed above, which provides sufficiently serious penalties for both cybercrime and breach of the data protection law, **Law No. 2008-08 on Electronic Transactions**, are, again, particularly welcome and significant pieces of legislation in light of the emerging presence of the internet as a medium of communication, conducting business, and dissemination of information in Senegal.

[13] See US Department of State, 2010 Human Rights Report: Senegal, 11th April 2011, available at: http://www.state.gov/j/drl/rls/hrrpt/2010/af/154366.htm

Recommendations

We recommend that the Senegalese government:

- Ensure that the rights of mobile telephony subscribers in relation to their personal data are guaranteed, in accordance with Law No. 2008-2012 on the Protection of Personal Data;

- Modify Article 7 of Law No. 2001-15 (containing the telecommunications code) to account for the rights of mobile telephony subscribers;

- Ensure that Law No 2008-2012 on the Protection of Personal Data is applied and respected in relation to the use of landing cards and biometric registration of passengers at Dakar airport;

- Replace the current system of collecting landing cards with a more effective collection mechanism, which provides more justification for, and greater transparency concerning, the various data fields being collected;

- Ensure sufficient budgetary allocation to the CPDP (Commission de Protection des Données Personnelles) to enable its effective operation;

- Investigate claims that illegal telephone monitoring is routinely undertaken by the security services, and ensure that such practices are stopped and responsible individuals held to account if the claims are verified.