COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 25 November / novembre 2015 T-PD(2015)01Bil

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL [STE n°108]

(T-PD)

COMPILATION OF OPINIONS

COMPILATION DES AVIS

Directorate General of Human Rights and Rule of Law /

Direction Générale Droits de l'Homme et Etat de droit

INDEX / TABLE DES MATIERES

Opinion on the Recommendation 2067 (2015) of the Parliamentary Assembly of the Council of Europe "Mass surveillance" (T-PD(2015)13)

1. The Ministers' Deputies agreed at their 1227th meeting (12 May 2015) to communicate to the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) the Recommendation 2067 (2015) on Mass surveillance, for information and possible comments by 12 July 2015.

2. The T-PD welcomes the adoption by the Parliamentary Assembly of the Recommendation 2067 (2015) which emphasises the importance of addressing the issue of surveillance practices that endanger fundamental human rights, including the right to privacy. It further welcomes the work of the Rapporteur.

3. The T-PD notes that, while the Recommendation "invites the Committee of Ministers to make use of the tools at its disposal to uphold the fundamental right to privacy in all member and observer States of the Council of Europe" it does not specifically refer to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). The T-PD recalls that the fundamental right to respect for private life is protected under Article 8 of the European Convention on Human rights, as well as under Convention 108 and its Additional Protocol, which is, to date, the only legally binding international instrument protecting individuals with regard to the processing of their personal data, thereby contributing to respect for their human rights and fundamental freedoms, and in particular their right to privacy and the protection of their personal data. The modernisation work of the Convention, which is now at its final stage, should strengthen the effectiveness of this tool at global level.

In this respect, T-PD invites the Council of Europe to step up its efforts for the promotion of Convention 108, in view of the accession of third countries and in particular those which already Parties to the Convention on Cybercrime.

4. In relation to paragraph 2.1, the T-PD welcomes the call for a recommendation to member states to ensure the protection of privacy in the digital age and Internet safety in the light of the threats posed by the mass surveillance techniques and stands ready to contribute to any future work in the area of its expertise. It highlights, in this respect, the Council of Europe Guide to Human Rights for Internet Users, and its implementation through capacity building and cooperation assistance activities. The Guide states that Internet users must not be subjected to general surveillance or interception measures but may only be subject to legitimate interference which is prescribed by law, such as a criminal investigation. In particular, users should have access to clear and precise information about the relevant law or policy and rights in this regard.

5. The T-PD welcomes the call made to member states in paragraph 2.2 to explore internet security issues related to mass surveillance and intrusion practices. Inviting all institutions and companies that process personal data, to apply the most effective security measures available, upholds the provisions of article 7 of Convention 108, which requires from member states to take appropriate security measures for the protection of personal data according to their vulnerability. Indeed, the processing of personal data engages the responsibility of all users, both in the public and private sector. While the processing of personal data by electronic means may prove to be highly beneficial for users, it may also raise concerns and undermine the position of the persons whose data are being processed.

Moreover, the text of the modernised Convention, in its article 7.2, contains a specific obligation for the data controller to notify without delay, at least to the competent supervisory authority, the data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

6. The T-PD welcomes the initiative of the Parliamentary Assembly to draw the attention of member states on exploring the threats posed by mass surveillance and intrusion practices, particularly in terms of human rights and fundamental freedoms. The T-PD recalls that, in the absence of any oversight mechanism, the processing of personal data may undermine the enjoyment of other fundamental rights

(the right to privacy, the right to non-discrimination and right to a fair trial) as well as other legitimate interests.

In order to maintain the balance between these various rights, Convention 108 imposes conditions and restrictions on the processing of personal data. While surveillance can be considered as being justified in the current context, this should not result in the de facto denial of the fundamental right to privacy for the protection of national security, as being an overriding public interest.

Furthermore, the T-PD recalls that in order to ensure respect for the rights of the persons concerned, Convention 108 and its Additional Protocol provide for the establishment of a national independent supervisory authority, with powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of the domestic law in relation to the protection of personal data. Parties, according to the Convention, further undertake to establish appropriate sanctions and remedies for violations of the provisions of domestic law giving effect to the basic principles of data protection.

In this context, the T-PD supports the call of the Parliamentary Assembly in paragraph 2.3, for the creation of an "intelligence codex" addressed to the intelligence services of all participating States and other third countries, which would define the principles of cooperation for the fight against terrorism and organised crime. Such an initiative regulating and defining clear and concrete rules is more than necessary in order to avoid any attempt of abuse. The T-PD is disposed and available to contribute in any future work if requested.

7. Finally, it is recalled that the T-PD addressed a letter to the chair of the Ministries' Deputies in December 2013, denouncing the use of mass surveillance techniques and suggesting that a line of action based on Convention 108 be defined in the field.

Avis sur la Recommandation 2067 (2015) de l'Assemblée Parlementaire du Conseil de l'Europe « Les opérations de surveillance massive » (T-PD(2015)13)

1. Les Délégués des Ministres ont décidé, à leur 1227e réunion (12 mai 2015), de communiquer au Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) la Recommandation 2067 (2015) intitulée « Les opérations de surveillance massive », pour information et commentaires éventuels avant le 12 juillet 2015.

2. Le T-PD se réjouit de l'adoption, par l'Assemblée parlementaire, de la Recommandation 2067 (2015), qui souligne l'importance de traiter la question des pratiques de surveillance mettant en danger des droits de l'homme fondamentaux, dont le droit au respect de la vie privée. Il salue, en outre, le travail du rapporteur.

3. Le T-PD note que, si la Recommandation « invite le Comité des Ministres à faire usage des *instruments* dont il dispose pour défendre le droit fondamental au respect de la vie privée dans l'ensemble des Etats membres et observateurs du Conseil de l'Europe », elle ne fait cependant pas explicitement référence à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108). Le T-PD rappelle que le droit fondamental au respect de la vie privée est protégé par l'article 8 de la Convention européenne des droits de l'homme, ainsi que par la Convention n° 108 et son protocole additionnel, qui est, à ce jour, le seul instrument international juridiquement contraignant à protéger les individus à l'égard du traitement de leurs données à caractère personnel ; la Convention n° 108 contribue ainsi au respect de leurs droits de l'homme et de leurs libertés fondamentales, et en particulier de leur droit au respect de la vie privée et la protection des données à caractère personnel. Le travail de modernisation de cette convention, qui est maintenant entré dans sa dernière phase, devrait renforcer l'efficacité de cet outil au niveau mondial.

   A cet égard, le T-PD invite le Conseil de l'Europe à redoubler d'efforts pour promouvoir la Convention n° 108, en vue de l'adhésion de pays tiers, notamment de ceux qui sont déjà Parties à la Convention sur la cybercriminalité.

4. Concernant le paragraphe 2.1, le T-PD se félicite de l'appel à adresser une recommandation aux Etats membres en vue de garantir la protection de la vie privée à l'ère du numérique et la sécurité d'internet à la lumière des menaces que représentent les techniques de surveillance massive ; il est prêt à contribuer à tous travaux futurs dans son domaine de compétence. Dans ce contexte, le T-PD fait référence au Guide des droits de l'homme pour les utilisateurs d'internet, ainsi qu'à sa mise en œuvre au moyen d'activités de renforcement des capacités et d'activités de coopération et d'assistance. Selon le guide, les utilisateurs d'internet ne doivent pas être soumis à des mesures générales de surveillance ou d'interception des communications ; ils peuvent cependant faire l'objet d'une ingérence légitime, prévue par la loi, par exemple dans le cadre d'enquêtes pénales. En particulier, les utilisateurs doivent avoir accès à des informations claires et précises, qui leur permettent de connaître les règles et la législation en vigueur, ainsi que leurs droits à cet égard.

5. Le T-PD de réjouit de l'appel, adressé aux Etats membres au paragraphe 2.2, à étudier les problèmes de sécurité sur internet que posent les pratiques de surveillance massive et d'intrusion. Inviter toutes les institutions et entreprises qui traitent des données à caractère personnel à appliquer les mesures de sécurité les plus efficaces qui soient disponibles est un moyen de promouvoir la mise en œuvre de l'article 7 de la Convention n° 108, qui impose aux Etats membres de prendre des mesures de sécurité appropriées pour la protection des données à caractère personnel, en fonction de leur vulnérabilité. De fait, le traitement de données à caractère personnel engage la responsabilité de tous les utilisateurs, dans le secteur public comme dans le secteur privé. Si le traitement de données à caractère personnel par des moyens électroniques peut présenter de grands avantages pour les utilisateurs, il peut aussi susciter des inquiétudes et fragiliser la situation des personnes dont les données sont traitées.

De plus, le texte de la Convention modernisée contient, à l'article 7.2, l'obligation spécifique, pour le responsable du traitement, de notifier, sans délai excessif, à tout le moins aux autorités de contrôle compétentes, les violations des données susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées.

6. Le T-PD se réjouit que l'Assemblée parlementaire ait pris l'initiative d'attirer l'attention des Etats membres sur l'importance d'étudier les menaces que représentent les pratiques de surveillance massive et d'intrusion, notamment sous l'angle des droits de l'homme et des libertés fondamentales. Le T-PD rappelle que, en l'absence de tout mécanisme de contrôle, le traitement de données à caractère personnel risque de compromettre la jouissance d'autres droits fondamentaux (droit au respect de la vie privée, droit à la protection contre la discrimination et droit à un procès équitable), ainsi que d'autres intérêts légitimes.

   En vue de maintenir l'équilibre entre ces différents droits, la Convention n° 108 soumet le traitement des données à caractère personnel à certaines conditions et restrictions. Si une surveillance peut être considérée comme justifiée dans le contexte actuel, cela ne doit cependant pas conduire à priver en pratique les individus du droit fondamental au respect de la vie privée au nom de l'intérêt public supérieur que constitue la protection de la sécurité nationale.

   En outre, le T-PD rappelle que, afin de garantir le respect des droits des personnes concernées, la Convention n° 108 et son protocole additionnel prévoient la création d'une autorité de contrôle indépendante au niveau national, investie de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations des dispositions du droit interne en relation avec la protection des données à caractère personnel. Selon la Convention, chaque Partie s'engage aussi à établir des sanctions et recours appropriés visant les violations des dispositions du droit interne donnant effet aux principes de base de la protection des données.

   Dans ce contexte, le T-PD soutient l'appel, lancé par l'Assemblée parlementaire au paragraphe 2.3, à créer un « code du renseignement » destiné aux services de renseignement de tous les Etats participants et de pays tiers, qui définisse les principes régissant la coopération aux fins de lutte contre le terrorisme et la criminalité organisée. Une telle initiative de régulation et de définition de règles claires et concrètes est plus que nécessaire pour éviter toute tentative d'abus. Le T-PD est disponible et prêt à contribuer à tous travaux futurs s'il y est invité.

7. Enfin, il est rappelé que le T-PD a adressé une lettre au président des Délégués des Ministres en décembre 2013, pour dénoncer l'utilisation des techniques de surveillance massive et suggérer que soit définie en la matière une ligne d'action fondée sur la Convention n° 108.

Opinion on the request for accession of Tunisia (Document T-PD(2015)14)

Introduction

By letter dated 6 July 2015, registered on 3 August 2015 at the Secretariat of the Council of Europe, the Tunisian Minister of Foreign Affairs expressed the Republic of Tunisia's interest in being invited to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108") and its Additional Protocol regarding supervisory authorities and transborder data flows.

The Consultative Committee of Convention 108 (T-PD) points out that it invited the Committee of Ministers in 2008 to take note of its recommendation to allow non-member states with data protection legislation in accordance with Convention 108 to accede to this Convention. The Ministers' Deputies took note of this recommendation and agreed to examine every accession request in the light of that recommendation (1031st meeting, 2 July 2008).

Opinion

In accordance with Article 4 of Convention 108, each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in the Convention (Chapter II). Pursuant to Article 3.1 of the Additional Protocol, the Parties shall regard the provisions of Articles 1 and 2 of the Protocol as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

Having examined the Constitution promulgated on 27 January 2014 and the relevant legislation (Institutional Act No. 2004-63 of 27 July 2004 on personal data – hereinafter the "Data Protection Act"), the T-PD notes the following.

1. Object and purpose (Article 1 of Convention 108)

Article 24 of the Constitution provides: "The state protects the right to privacy and the inviolability of the home, and the confidentiality of correspondence, communications, and personal information". Article 1 of the Data Protection Act sets out its object and purpose: "Everyone has the right to the protection of personal data relating to his or her private life as one of the fundamental rights guaranteed by the Constitution. The processing of personal data shall comply with the principles of transparency, fairness and respect for human dignity, in accordance with the provisions of this Act."

While Article 1 of the Data Protection Act is in the spirit of the Convention, it should be noted that Article 1 of Convention 108, the aim of which is to secure for every individual "respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')", is a means of protecting an individual with regard to the processing of personal data other than those "relating only to their private life" and that this limitation in the Tunisian Act should consequently be reviewed.

2. Definitions

a) Personal data (Article 2.a of Convention 108)

Article 4 of the Data Protection Act defines personal data as "any information, whatever its origin or its form, relating to an individual who can be identified either directly or indirectly, with the exception of information relating to public life or considered as such by the law".

This definition is more detailed than the wording of Convention 108 and corresponds to the definition given in Article 2.a of the Convention, but with the exclusion of a category of information ("relating to public life)" that

should in pursuance of Convention 108 fall within the scope of the definition of personal data and accordingly be accorded the corresponding protection (provided there is no conflict with the right to freedom of expression, which, when several conditions are met, authorises a restriction on the right to respect for privacy).

b) Automated data file (Article 2. b of Convention 108)

Article 6 of the Data Protection Act defines the "data file" as "any structured and collated set of personal data that may be consulted in accordance with specific criteria that enable a particular person to be identified".

This definition is narrower than that of Convention 108, which states that "automated data file means any set of data undergoing automatic processing". The Data Protection Act uses the concept of "consultation" rather than "processing".

c) Automated processing (Article 2.c of Convention 108)

Article 6 of the Data Protection Act defines the processing of personal data as consisting of "manual or automated operations carried out by an individual or legal entity, with the aim of obtaining, recording, storing, organising, altering, exploiting, using, sending, distributing, disseminating, destroying or consulting personal data, as well as any operation in relation to the use of databases, indexes, directories, data files or the interconnection thereof".

The definition of processing in the Data Protection Act corresponds to the one given in Article 2.c of Convention 108 but without emphasising the application of logical and/or arithmetical operations to data, which is covered by the terms data exploitation and use. The Data Protection Act adds to the non-exhaustive list in Convention 108 a number of operations, including manual operations, such as interconnection (which is also defined), indexes and directories.

d) Controller (Article 2.d of Convention 108)

The definition of the controller is provided in Article 6 of the Data Protection Act: "any individual or legal entity that determines the aims and means of the processing of personal data".

This definition does not expressly mention the public authorities, in contrast to Convention 108, the scope of which covers both the private and the public sector. Section 1 of Chapter V, on specific processing categories, deals with the processing of personal data by public entities (Article 53 to 61 of the Act) and sets out a system of exceptions.

Section 2 of the Data Protection Act describes precisely and in considerable detail the obligations of the controller (or, as the case may be, the processor, who is also defined in Article 6).

3. Scope of the data protection system (Article 3 of Convention 108)

The Data Protection Act contains no details of its scope of application.

Having regard to the Convention, the Tunisian legislation, the scope of which appears considerably more limited, should specify and stipulate the scope of the Data Protection Act, which should be identical for processing carried out by both the private and the public sector.

In addition, Article 16 of the Act, relating to the processing of data concerning the employee's work situation, seems to establish a system of exceptions, which should not be the case.

4. Quality of data (Article 5 of Convention 108)

Article 9 of the Data Protection Act sets out the fundamental principles according to which the processing of personal data must be carried out: “The processing of personal data shall be carried out with due respect for human dignity, privacy and public freedoms”.

The same Article states that “[t]he processing of personal data, whatever its origin or form, shall not violate the human rights protected by the laws and regulations in force. In all cases, the use of personal data with the aim of breaching the rights or damaging the reputation of individuals shall be prohibited”.

Articles 10 and 11 of the Data Protection Act give effect to the fundamental principles of data protection, such as limiting the purposes for which it may be carried out (Article 10: “The collection of personal data shall be carried out exclusively for lawful, specific and explicit purposes”). Moreover, Article 17 contains a strict ban on “providing services to or giving an advantage to persons in return for their consent to the processing of their personal data or the use of their personal data for purposes other than those for which they have been collected”.

The Act also mentions conditions relating to quality and proportionality (Article 11): “Personal data shall be processed honestly and within the limits necessary to achieve the purpose for which they have been collected”.

Article 11 of the Act also states that the data controller shall ensure that the data are accurate, precise and up-to-date.

Generally speaking, the principles mentioned in Articles 9 to 11 of the Data Protection Act are in line with the provisions of Convention 108. Article 12 provides for an exception for the collection of data “if the processing is essential for particular scientific purposes” (Article 12 in conjunction with Articles 66 to 68). As far as this exclusion is concerned, it is recommended that reference be made to the relevant legislation or that new legislation be passed, if such is not already the case, specifying and governing these forms of processing. Clear mention should also be made of the legitimate grounds for any processing (law, contract, consent, etc), whereas this is only laid down in the case of subsequent processing operations (Article 12 of the Act).

5. Special categories of data (Article 6 of Convention 108)

Articles 13 and 14 of the Data Protection Act prohibit the processing of data “relating to offences, convictions, criminal prosecutions, sentences, preventive measures and criminal records, as well as data concerning, “directly or indirectly, racial or genetic origin, religious beliefs, political or philosophical views, trade union membership or health”.

The Act also provides for exceptions to this prohibition. For example, the data in question may be processed if the data subject has given his or her explicit consent by any means leaving a written record, if these data have clearly entered the public domain or if the processing is necessary for historical or scientific purposes or for the protection of the data subject’s vital interests.

Article 15 states that the processing of the data in question is subject to the authorisation of the National Personal Data Protection Authority, with the exception of data relating to health.

Articles 62 to 65 also contain provisions on the processing of health data (Chapter V of the Act, Specific processing categories).

Articles 13, 14 and 15 and Chapter V of the Data Protection Act (Articles 62 to 65 on the processing of health data, and Articles 66 to 68 in connection with scientific research) refer to the fundamental principle of prohibiting the processing of sensitive data, together with the possible exceptions and the generally appropriate safeguards, albeit reduced with regard to health data. These safeguards, provided for in Articles

12 and 14, may, on the whole, be considered to be in compliance with the provisions of Convention 108, with the exception of the processing of data on the sexual lives of the persons concerned, which is not the subject of any specific additional safeguards such as those provided by Article 6 of Convention 108, and with the exception of Chapter V, in which the reduced system of exceptions may prove insufficient. The processing of sensitive data by public entities is not covered by any specific system of protection and therefore fails to meet the requirements of Convention 108.

In addition, at the end of this list of exceptions to the prohibition of processing personal data the Act provides for the possibility of an exception when the data have "clearly entered the public domain or if the processing is necessary for historical or scientific purposes". As far as these eventualities are concerned, it is recommended that they be clarified or that specific legislation be passed, if such is not already the case.

6. Data security (Article 7 of Convention 108)

In accordance with Articles 18 to 21 of the Data Protection Act, the data controller (and the processor, under Article 20) must implement appropriate technical and structural measures to ensure the security of personal data against accidental or unauthorised destruction, accidental loss, unauthorised access, alteration or dissemination, as provided for by Article 7 of Convention 108.

Articles 18 to 21 of the Data Protection Act comply with the requirements of Article 7 of Convention 108.

7. Right to information (Article 8.a of Convention 108)

Article 31 sets out the information that must be notified to data subjects before their personal data are processed.

"- the nature of the personal data covered by the processing;

- the purposes of the processing of the personal data;

- whether replies to the questions are compulsory or optional;

- the consequences of any failure to reply;

- the name of the individual or legal entity in receipt of the data or the name and address of the individual or legal entity that has right of access;

- the surname and first name or the company name of the data controller and, where applicable, the name and address of the data controller's representative;

- their right of access to the data relating to them;

- their right to withdraw their consent to the processing at any time;

- their right to object to the processing of their personal data;

- the period of storage of personal data;

- a summary of the steps taken to guarantee the security of personal data;

- the country to which the data controller may intend to transfer the personal data.

The notification must be made by registered letter with acknowledgement of receipt or by any other means leaving a written record at least one month prior to the date scheduled for the processing of personal data."

The wording of these provisions complies with the requirements of Article 7 of Convention 108.

8. Additional safeguards for the data subject (Article 8.b to d of Convention 108)

The Data Protection Act provides for the right to object (Articles 42 and 43), the right of access (Articles 32 to 41), the right to rectification (Article 40, and data controller's obligation in Article 21) and the right of deletion (Article 45).

a) Right of access:

Article 32 states that "the right of access shall be understood as the right of the data subject to consult all the personal data relating to him or her as well as the right to correct, complement, rectify, update, modify, clarify or delete the data where they prove inaccurate or ambiguous or where the processing of such data is prohibited. The right of access shall also cover the right to obtain an accurate copy of the personal data in clear language and in an intelligible form where the data are processed by automated means".

Article 34 provides that the right of access may be exercised "by the data subject, his or her heirs or guardian". While it may appear normal that this right be exercised by a legal representative in certain circumstances, care should be taken to ensure that the rights of data subjects are safeguarded.

It should be noted that this right is not always applicable where data are processed by public entities.

b) Right to object:

In accordance with Article 42 of the Data Protection Act, any data subject "has the right to object to the processing of personal data related to him or her […], except where the processing is provided for by law or is required by the nature of the obligation. Furthermore, the data subject […] (has) the right to object to these data […] being communicated to third parties in order to enable them to be exploited for promotional purposes".

c) Right of rectification and deletion:

- Rectification

Article 40 provides that "[t]he data subject may request that personal data relating to them be rectified, supplemented, modified, clarified, updated and deleted where they prove inaccurate, incomplete or ambiguous or to ask for the data to be destroyed where their collection or use is in breach of this Act".
The Act also provides for the possibility for data subjects to "request, free of charge, […] a copy of the personal data and to indicate what action has not been carried out in respect of these data".

- Deletion

Article 45 provides that "personal data shall be destroyed as soon as the specified storage period has expired".

d) Right of appeal

Article 38 provides that "if the data controller or the sub-contractor [*processor*] refuses to allow the data subject to consult his or her personal data or postpones access to these data or refuses to issue a copy of these data, the data subject, his or her heirs or guardian may apply to the [National Personal Data Protection] Authority within one month of the refusal."

The T-PD notes that a number of matters could be clarified: 1) the criteria applicable for determining the existence (or otherwise) of a fee for exercising the right of access; 2) the current amount of the fee, in order for an assessment to be made as to whether it satisfies the criterion laid down in Convention 108 ("without excessive […] expense"); 3) whether this fee is reimbursed to the data subject if the data are imprecise or the processing is unlawful; 4) the Act says nothing about the deadlines by which the data controller must comply with the request. This needs to be clarified in order for an assessment to be made as to whether the deadline

satisfies the criterion laid down in Article.8 b of Convention 108 (access to these data must be obtained "without excessive delay").

Overall, the additional safeguards meet the requirements of Convention 108.

9. Exceptions and restrictions (Article 9 of Convention 108)

Chapter V. of the Data Protection Act sets out a system of exceptions where processing is carried out by public entities "in connection with public security, national defence or criminal prosecutions or where the said processing proves necessary" for carrying out public service duties in pursuance of the laws in force.

This system of exceptions seems too broad insofar as no qualifying details are provided with regard to the actual purpose of the processing and as there are no additional safeguards for the processing of sensitive data.

The T-PD believes it necessary to clarify the compatibility between freedom of expression and the protection of privacy in order to comply with the principle laid down in Article 9.2.b of Convention 108.

10. Sanctions and remedies (Article 10 of Convention 108)

The Data Protection Act (Articles 86 to 103) specifies the penalties applicable to breaches of the Act. These provisions meet the requirements of Article 10 of Convention 108.

11. Transborder data flows (Article 12 of Convention 108 and Article 2 of the Additional Protocol)

Article 51 of the Data Protection Act provides: "The transfer to another country of personal data […] may not take place except where that country ensures an adequate level of protection, which is to be assessed in the light of the nature of the data to be transferred, the purposes of the processing, the period scheduled for the processing, the country to which the data are to be transferred and the requisite precautions taken to ensure data security". Such transfer is also subject to compliance with the conditions laid down by the Data Protection Act.

In addition, Article 50 of the Act prohibits, in a general way, "communicating or transferring personal data abroad where such communication or transfer may endanger public security or harm Tunisia's vital interests".

Overall, these provisions meet the criteria set out in Convention 108 and the Additional Protocol.

Article 52 of the Act also provides that "[i]n all cases, the authorisation of the [National Personal Data Protection] Authority shall be required for the transfer of personal data abroad".

12. Supervisory authority (Article 1 of the Additional Protocol)

Article 75 of the Data Protection Act establishes the National Personal Data Protection Authority, which is the supervisory body responsible for ensuring compliance with the principles applying to the processing of personal data. Decree No. 2007-3003 of 27 November 2007 lays down the Authority's operating procedures.

The same Article provides that this institution is financially independent as its budget is part of that of the ministry with responsibility for human rights.

These provisions are in conformity with Article 1.1 of the Additional Protocol to the Convention.

Furthermore, Article 79 provides guarantees of impartiality with regard to the Authority's internal functioning: "It is prohibited for the President of the Authority and its members to hold any direct or indirect interest in any firm involved in the processing of personal data, whether automated or manual".

With regard to guarantees of institutional independence and in order to be fully compliant with Article 1.3 of the Additional Protocol, which stipulates that "[t]he supervisory authorities shall exercise their functions in complete independence", Tunisian legislation should clearly establish the Authority's independence and clarify its legal status, as well as the conditions relating to the renewal or dismissal of the members of the Authority.

Article 77 establishes the Authority's powers of investigation, authorisation and intervention as well as its duty "to inform the public prosecutor in the relevant jurisdiction about any offences that have come to its notice in the course of its work".

These provisions are in line with Article 1.2.a of the Additional Protocol.

Article 76 gives the National Personal Data Protection Authority the power to receive complaints in connection with the Data Protection Act. However, the Act does not state whether this remedy is open to all persons concerned or whether it is limited, and whether persons outside the country could also file a complaint or not. In order to ensure the conformity of this provision with the Additional Protocol, which requires that the supervisory authority "shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data", Tunisian legislation should clarify the arrangements for this referral.

Article 82 provides for the possibility of lodging an appeal to a court (the Tunis Court of Appeal and the Court of Cassation) against the Authority's decisions.

Overall, these provisions meet the requirements of Convention 108 and the Additional Protocol (Article.1.4).

Additional considerations

It should be noted that:

- There are a number of additional definitions of notions such as: third party, beneficiary, communication, interconnection, and processor.

- There are additional obligations concerning the preliminary procedures for processing personal data (Article 7, which provides that "any operation for processing personal data must be previously notified to the National Authority [...] at its head office").

- Article 22 contains additional conditions to be met by the controller. The Committee questions the applicability and consequences of the condition relating to the Tunisian nationality of the controller.

- Articles 69 to 74 govern the processing of personal data for video surveillance purposes.

Conclusion

In the light of the foregoing, the T-PD considers that the Tunisian Data Protection Act generally heads towards the principles giving effect to Convention 108 and its Additional Protocol, although several modifications are necessary to bring it into full conformity, and recommends that the Committee of Ministers invites the Republic of Tunisia to accede to both instruments, once it has complied with the observations set out above.

Avis sur la demande d'adhésion de la Tunisie (Document T-PD(2015)14)

Introduction

Par lettre du 6 juillet 2015, enregistrée le 3 août 2015 au Secrétariat Général du Conseil de l'Europe, le Ministre des affaires étrangères de la Tunisie a exprimé l'intérêt de la République tunisienne d'être invitée à adhérer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après, la « Convention 108 ») et à son Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données.

Le Comité consultatif de la Convention 108 (T-PD) rappelle qu'il avait invité en 2008 le Comité des Ministres à prendre acte de sa recommandation visant à autoriser à adhérer à la Convention 108 les Etats non membres ayant en matière de protection des données une législation conforme à cette Convention. Les délégués des ministres avaient pris acte de cette recommandation et décidé d'examiner toute demande d'adhésion à la lumière de celle-ci (1031ème réunion – 2 juillet 2008).

Avis

Conformément à l'article 4 de la Convention 108, chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans la Convention (Chapitre II). En vertu de l'article 3.1 du Protocole additionnel, les Parties considèrent les dispositions des articles 1 et 2 du Protocole comme des articles additionnels à la Convention, et toutes les dispositions de la Convention s'appliquent en conséquence.

Après avoir examiné la Constitution promulguée le 27 janvier 2014 et la législation pertinente (Loi organique n° 2004-63 du 27 juillet 2004 portant sur les données à caractère personnel, ci-après « la loi sur la protection des données »), le T-PD constate ce qui suit :

1. Objet et but (article 1er de la Convention 108)

L'article 24 de la Constitution dispose que « l'Etat protège la vie privée, l'inviolabilité du domicile et la confidentialité des correspondances, des communications et des données personnelles ». La loi sur la protection des données définit quant à elle à son article premier son objet et sa finalité : « toute personne a le droit à la protection des données à caractère personnel relatives à sa vie privée comme étant l'un des droits fondamentaux garantis par la Constitution et ne peuvent être traitées que dans le cadre de la transparence, la loyauté et le respect de la dignité humaine et conformément aux dispositions de la présente loi. »

Si l'article 1er de la loi sur la protection des données s'inscrit dans l'esprit de la Convention 108, il convient de noter que l'article 1er de la Convention 108, qui vise à garantir à toute personne physique « le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données ») » permet quant à lui de protéger une personne au regard du traitement de données personnelles autres que celles « purement relatives à sa vie privée » et que cette limitation dans la loi tunisienne devrait en conséquence être revue.

2. Définitions

a) Données à caractère personnel (article 2.a de la Convention 108)

La loi sur la protection des données définit à son article 4 les données à caractère personnel comme « toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou

indirectement d'identifier une personne physique ou la rendent identifiable, à l'exception des informations liées à la vie publique ou considérées comme telles par la loi. »

Cette définition, qui est plus détaillée que le libellé de la Convention 108, correspond à la définition donnée à l'article 2.a de cette dernière, avec toutefois l'exclusion d'une catégorie d'informations (celles «liées à la vie publique») qui devrait au sens de la Convention 108 rentrer dans la définition des données personnelles et donc faire l'objet de la protection correspondante (sous–réserve de l'absence de conflit avec le droit à la liberté d'expression, qui permet lorsque plusieurs conditions sont satisfaites d'obtenir une limitation du droit au respect de la vie privée).

b) Fichier automatisé (article 2. b de la Convention 108)

La loi sur la protection des données définit à son article 6 le «fichier » comme étant l'« ensemble des données à caractère personnel structuré et regroupé, susceptible d'être consulté selon des critères déterminés et permettant d'identifier une personne déterminée.»

Cette définition est plus restreinte que celle de la Convention 108, qui prévoit que le « fichier automatisé signifie tout ensemble d'informations faisant l'objet d'un traitement automatisé ». La loi sur la protection des données utilise la notion de « consultation » plutôt que celle de « traitement ».

c) Traitement automatisé (article 2.c de la Convention 108)

L'article 6 de la loi sur la protection des données définit le traitement des données à caractère personnel comme étant constitué des « opérations réalisées d'une façon automatisée ou manuelle par une personne physique ou morale, et qui ont pour but notamment la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation, l'utilisation, l'expédition, la distribution, la diffusion ou la destruction ou la consultation des données à caractère personnel, ainsi que toutes les opérations relatives à l'exploitation de bases des données, des index, des répertoires, des fichiers, ou l'interconnexion ».

La définition du traitement dans la loi sur la protection des données correspond à la définition qui se trouve à l'article 2.c de la Convention 108, sans toutefois souligner l'application d'opérations logiques et/ou arithmétiques aux données, cela étant couvert par les notions d'exploitation et d'utilisation des données. La loi sur la protection des données ajoute un certain nombre d'opérations, y compris manuelles, à la liste non exhaustive de la Convention 108, comme l'interconnexion (qui est par ailleurs également définie), des index ou des répertoires.

d) Responsable du traitement / Maître du fichier (article 2.d de la Convention 108)

La définition du responsable du traitement/maître du fichier est donnée à l'article 6 de la loi sur la protection des données. Elle désigne : « toute personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel. »

Cette définition ne mentionne pas de façon expresse les autorités publiques comme le fait la Convention 108 dont le champ d'application couvre tant le secteur privé que le secteur public. La première section du Chapitre V dédié aux catégories particulières de traitement traite du traitement de données personnelles par des personnes publiques (articles 53 à 61 de la loi), établissant un régime dérogatoire.

La Section 2 de la loi sur la protection des données décrit de manière très détaillée et précise les obligations qui incombent au responsable du traitement (le cas échéant au sous-traitant, qui est également défini à l'article 6).

3. Champ d'application du régime de protection des données (article 3 de la Convention 108)

La loi sur la protection des données ne prévoit pas de définition de son champ d'application.

Eu égard à la Convention, il serait souhaitable que la législation tunisienne, dont le champ paraît nettement plus restreint, précise et détermine le champ d'application de la loi sur la protection des données, qui soit un champ d'application uniforme pour les traitements effectués par le secteur privé et par le secteur public.

Par ailleurs, l'article 16 de la loi, relatif au traitement de données concernant la situation professionnelle de l'employé semble établir un régime dérogatoire qui n'a pas lieu d'être.

4. Qualité des données (article 5 de la Convention 108)

L'article 9 de la loi sur la protection des données énumère les principes fondamentaux à la lumière desquels doit s'effectuer le traitement des données personnels. « Le traitement des données à caractère personnel doit se faire dans le cadre du respect de la dignité humaine, de la vie privée et des libertés publiques. »

Le même article précise que « le traitement des données à caractère personnel, quelle que soit son origine ou sa forme, ne doit pas porter atteinte aux droits des personnes protégées par les lois et les règlements en vigueur, et il est, dans tous les cas, interdit d'utiliser ces données pour porter atteinte aux personnes ou à leur réputation. »

Les articles 10 et 11 de la loi sur la protection des données donnent effet aux principes fondamentaux de la protection des données tels que la limitation des finalités (art.10 « La collecte des données à caractère personnel ne peut être effectuée que pour des finalités licites, déterminées et explicites »). De plus, l'article 17 prévoit une interdiction formelle « de lier la prestation d'un service ou l'octroi d'un avantage à une personne à son acceptation du traitement de ses données personnelles ou de leur exploitation à des fins autres que celles pour lesquelles elles ont été collectées.»

La loi formule également les conditions tenant à la qualité et la proportionnalité (article 11). « Les données à caractère personnel doivent être traitées loyalement, et dans la limite nécessaire au regard des finalités pour lesquelles elles ont été collectées. »

L'article 11 de la loi prévoit également l'obligation pour le responsable du traitement de s'assurer de l'exactitude, précision et mise à jour des données.

De manière générale, les principes énoncés aux articles 9 à 11 de la loi sur la protection des données sont conformes aux dispositions de la Convention 108. L'art.12 prévoit une exception pour la collecte de données « si le traitement mis en œuvre est nécessaire à des fins scientifiques certaines ». (Article 12 combiné aux articles 66 à 68). En ce qui concerne cette exclusion, il est recommandé de préciser ou d'adopter une législation spécifique précisant et encadrant ces formes de traitement, si tel n'est pas le cas. Par ailleurs, il conviendrait de mentionner clairement les bases de légitimité du traitement primaire (loi, contrat, consentement, etc.) alors que cela n'est prescrit que dans le cas de traitements ultérieurs (article 12 de la loi).

5. Catégories particulières de données (article 6 de la Convention 108)

La loi sur la protection des données prévoit aux articles 13 et 14 l'interdiction de traiter les données relatives « aux infractions, à leur constatation, aux poursuites pénales, aux peines, aux mesures préventives et aux antécédents judiciaires » ainsi que les données qui concernent « directement ou indirectement l'origine raciale ou génétique, les convictions religieuses, les opinions politiques, philosophiques ou syndicales, ou la santé ».

La loi prévoit également des exceptions à cette interdiction. Ainsi, le traitement des données visées peut s'effectuer avec le consentement exprès de la personne concernée, donné par n'importe quel moyen laissant une trace écrite, ou lorsque ces données ont acquis un aspect manifestement public, ou lorsque ce traitement s'avère nécessaire à des fins historiques ou scientifiques, ou lorsque ce traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée.

L'art.15 précise que le traitement des données concernées est soumis à l'autorisation de L'Instance Nationale de Protection des données à Caractère Personnel à l'exception des données relatives à la santé.

Les articles 62 à 65 contiennent par ailleurs des dispositions relatives au traitement des données de santé (Chapitre V de la loi, Catégories particulières de traitement).

Les articles 13,14 et 15 et le Chapitre V de la loi sur la protection des données (sur le traitement des données à caractère personnel relatives à la santé, articles 62 à 65 et dans le cadre de la recherche scientifique, articles 66 à 68) contiennent le principe fondamental de l'interdiction du traitement des données sensibles avec les exceptions possibles assorties des garanties généralement appropriées, bien que réduites concernant les données de santé. Ces garanties, prévues aux articles 12 et 14 peuvent être globalement considérées comme compatibles avec les dispositions de la Convention 108, à l'exception du traitement des données relatives à la vie sexuelle des personnes concernées, qui ne fait donc l'objet d'aucun régime de garanties complémentaires spécifiques comme le prévoit l'article 6 de la Convention 108, et du Chapitre V dont le régime dérogatoire réduit peut se révéler insuffisant. Le traitement de données sensibles par des personnes publiques ne bénéficie d'aucun régime de protection spécifique, ce qui n'est pas conforme aux exigences de la Convention 108.

Par ailleurs, au terme de ces exceptions à l'interdiction de traitement des données personnelles, la loi prévoit la possibilité d'exception quand les données ont acquis « un aspect manifestement public, ou lorsque ce traitement s'avère nécessaire à des fins historiques ou scientifiques ». En ce qui concerne ces possibilités, il est recommandé de préciser ces notions ou d'adopter une législation spécifique concernant ces hypothèses si tel n'est pas le cas.

6. Sécurité des données (article 7 de la Convention 108)

Conformément aux articles 18 à 21 de la loi sur la protection des données, le responsable du traitement (et le sous-traitant conformément à l'article 20) doit mettre en œuvre des mesures adéquates d'ordre technique et structurel pour assurer la sécurité des données à caractère personnel contre toute destruction accidentelle ou non autorisée, perte accidentelle, accès, modification ou diffusion sans autorisation, ainsi que le prévoit l'article 7 de la Convention 108.

Dans ces termes, les articles 18 à 21 de la loi sur la protection des données sont en conformité avec l'article7 de la Convention 108.

7. Droit d'information (article 8.a de la Convention 108)

L'article 31 énumère les informations qui doivent être communiquées à la personne concernée préalablement au traitement de ses données personnelles.

« - la nature des données à caractère personnel concernées par le traitement ;

- les finalités du traitement des données à caractère personnel ;

- le caractère obligatoire ou facultatif de leur réponse;

- les conséquences du défaut de réponse ;

- le nom de la personne physique ou morale bénéficiaire des données, ou de celui qui dispose du droit d'accès et son domicile ;

- le nom et prénom du responsable du traitement ou sa dénomination sociale et, le cas échéant, son représentant et son domicile ;

- leur droit d'accès aux données les concernant ;

- leur droit de revenir, à tout moment, sur l'acceptation du traitement ;

- leur droit de s'opposer au traitement de leurs données à caractère personnel ;

- la durée de conservation des données à caractère personnel ;

- une description sommaire des mesures mises en œuvre pour garantir la sécurité des données à caractère personnel ;

- le pays vers lequel le responsable du traitement entend, le cas échéant, transférer les données à caractère personnel. »

La notification s'effectue par lettre recommandée avec accusé de réception ou par n'importe quel moyen laissant une trace écrite dans un délai d'un mois au moins avant la date fixée pour le traitement des données à caractère personnel. »

Ces dispositions sont formulées en conformité avec les exigences de la Convention 108.

8. Garanties complémentaires pour la personne concernée (articles 8.b à 8.d de la Convention 108)

La loi sur la protection des données prévoit le droit d'opposition (articles 42 et 43), le droit d'accès (articles 32 à 41) ainsi que le droit de rectification (article 40 et obligation du responsable de traitement à l'article 21) et de suppression (article 45).

a) Le droit d'accès :

L'article 32 précise que l'on « entend par droit d'accès, le droit de la personne concernée, de consulter toutes les données à caractère personnel la concernant, ainsi que le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer lorsqu'elles s'avèrent inexactes, équivoques, ou que leur traitement est interdit. Le droit d'accès couvre également le droit d'obtenir une copie des données dans une langue claire et conforme au contenu des enregistrements, et sous une forme intelligible lorsqu'elles sont traitées à l'aide de procédés automatisés. »

L'article 34 prévoit que le droit d'accès peut être exercé « par la personne concernée, ses héritiers ou son tuteur ». S'il paraît normal que ce droit soit dans certaines circonstances exercé par un représentant légal, il convient néanmoins de veiller à ce que les droits des personnes concernées soient préservés.

Il convient de noter que ce droit n'est pas toujours applicable dans le cas de traitements de données par des personnes publiques.

b) Le droit d'opposition :

En vertu de l'article 42 de la loi sur la protection des données, toute personne concernée « a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant …sauf dans les cas où le traitement est prévu par la loi ou est exigé par la nature de l'obligation. En outre la personne concernée […] a le droit de s'opposer à ce que les données […] soient communiquées aux tiers en vue de les exploiter à des fins publicitaires. »

c) Le droit de rectification et de suppression :

- rectification

L'article 40 dispose que « la personne concernée, peut demander de rectifier les données à caractère personnel la concernant, les compléter, les modifier, les clarifier, les mettre à jour, les effacer lorsqu'elles s'avèrent inexactes, incomplètes, ou ambigües, ou demander leur destruction lorsque leur collecte ou leur utilisation a été effectuée en violation de la présente loi. »
En outre la loi prévoit la possibilité pour les personnes concernées de « demander, sans frais […] la délivrance d'une copie des données à caractère personnel et indiquer ce qui n'a pas été réalisé en ce qui concerne ces données. »

- Suppression

L'article 45 prévoit que « les données à caractère personnel doivent être détruites dès l'expiration du délai fixé à leur conservation ».

d) Le droit de recours :

L'article 38 prévoit que « dans le cas où le responsable du traitement ou le sous- traitant refuse de permettre à la personne concernée la consultation des données à caractère personnel requises, ou diffère l'accès à ces données, ou refuse de leur délivrer une copie de ces données, la personne concernée, ses héritiers ou son tuteur peuvent présenter une demande à l'Instance dans un délai maximum d'un mois à compter de la date du refus. »

Le T-PD constate qu'un certain nombre d'éléments pourraient être précisés : 1) les critères applicables à la détermination de l'existence de la redevance (ou pas) pour l'exercice du droit d'accès ; 2) le montant actuel éventuel de la redevance, afin que l'on puisse évaluer s'il satisfait au critère énoncé dans la Convention 108 : « sans […] frais excessifs » ; 3) si cette redevance est remboursée à l'intéressé en cas de données inexactes ou de traitement illicite ; 4) puis, la loi ne dit rien sur les délais dans lesquels le responsable du traitement doit satisfaire la demande. Cette précision devrait être apportée pour que l'on puisse évaluer si elle correspond au critère énoncé par la Convention 108, car l'art.8 b prévoit que l'accès à ces données doit être réalisé « sans délais […] excessifs ».

Dans l'ensemble, les garanties complémentaires correspondent aux exigences de la Convention 108.

9. Exceptions et restrictions (article 9 de la Convention 108)

Le Chapitre V de la loi sur la protection des données établit un régime dérogatoire pour les traitements effectués par des personnes publiques « dans le cadre de la sécurité publique ou de la défense nationale, ou pour procéder aux poursuites pénales, ou lorsque ledit traitement s'avère nécessaire » à l'exécution des missions de service public conformément aux lois en vigueur.

Ce régime dérogatoire semble trop large dans la mesure où aucune nuance n'est apportée en fonction de la finalité concernée et en raison de l'absence de garanties complémentaires pour le traitement des données sensibles.

Le T-PD fait observer qu'il convient de préciser la compatibilité entre d'une part, la liberté d'expression, et d'autre part, la protection de la vie privée afin de satisfaire au principe de l'article 9.2.b de la Convention 108.

10. Sanctions et recours (article 10 de la Convention 108)

La loi sur la protection des données (articles 86 à 103) établit les sanctions applicables en cas de violation des dispositions de la loi sur la protection des données. Ces dispositions sont conformes à l'article 10 de la Convention 108.

11. Flux transfrontières de données à caractère personnel (article 12 de la Convention 108 et article 2 de son Protocole additionnel)

La loi sur la protection des données prévoit dans son article 51 que « le transfert vers un autre pays des données personnelles […] ne peut avoir lieu que si ce pays assure un niveau de protection adéquat apprécié au regard de tous les éléments relatifs à la nature des données à transférer, aux finalités de leur traitement, à la durée du traitement envisagé, et le pays vers lequel les données vont être transférées ainsi que les précautions nécessaires mises en œuvre pour assurer la sécurité des données », ainsi que dans le respect des conditions prévues par la loi sur la protection des données.

De plus, l'article 50 de la loi interdit de manière générale, « de communiquer ou de transférer des données à caractère personnel vers un pays étranger lorsque ceci est susceptible de porter atteinte à la sécurité publique ou aux intérêts vitaux de la Tunisie. »

Ces dispositions correspondent globalement aux critères énoncés dans la Convention 108 et son Protocole additionnel.

L'article de la loi dispose par ailleurs que « dans tous les cas, l'obtention de l'autorisation de l'Instance pour effectuer le transfert des données à caractère personnel vers l'étranger est obligatoire. »

12. Autorités de contrôle (article 1 du Protocole additionnel)

L'article 75 de la loi sur la protection des données institue l'autorité de contrôle chargée de veiller au respect de principes de traitement des données personnelles dénommée « L'Instance Nationale de Protection des Données à Caractère Personnel » (INPDCP). Le Décret n° 2007-3003 du 27 novembre 2007, fixe par ailleurs les modalités de fonctionnement de l'INPDCP.

Le même article prévoit que cette institution jouit de l'autonomie financière, son budget étant rattaché au budget du ministère chargé des Droits de l'Homme.

Ces dispositions correspondent à l'article 1.1 du Protocole additionnel à la Convention.

De plus, l'article 79 prévoit des garanties d'impartialité concernant le fonctionnement interne de l'institution. Ainsi, « Il est interdit au président de l'Instance et à ses membres d'avoir, directement ou indirectement, des intérêts dans toute entreprise qui exerce ses activités dans le domaine du traitement des données à caractère personnel soit d'une façon automatisée, soit d'une façon manuelle. »

S'agissant des garanties d'indépendance institutionnelle et afin d'être pleinement conforme à l'article 1.3 du Protocole additionnel qui exige que « les autorités de contrôle exercent leurs fonctions en toute indépendance », la législation tunisienne devrait établir clairement l'indépendance de l'Instance et préciser son statut juridique ainsi que les conditions de reconduction et de destitution des membres de l'Instance.

L'article 77 prévoit les compétences d'investigation, d'autorisation, d'intervention, dont dispose l'INPDCP ainsi que son devoir « d'informer le procureur de la République territorialement compétent de toutes les infractions dont elle a eu connaissance dans le cadre de son travail ».

Ces dispositions sont conformes à l'article 1.2.a du Protocole additionnel.

L'article 76 donne à l'instance nationale de protection des données à caractère personnel la compétence de recevoir les plaintes portées dans le cadre de la loi sur la protection de données. Toutefois, la loi ne précise pas si ce recours est ouvert à toute personne concernée ou s'il est limité, ni si une telle plainte peut être introduite par une personne résidant à l'étranger. Afin d'assurer la conformité de cette disposition au Protocole additionnel, qui exige que l'autorité de contrôle puisse « être saisie par toute personne d'une

demande relative à la protection de ses droits et libertés fondamentales à l'égard du traitement de données » la concernant, il serait nécessaire que la législation tunisienne précise le cadre de cette saisine.

L'article 82 prévoit la possibilité de recours juridictionnel contre les décisions de l'Instance (devant la Cour d'appel de Tunis ainsi que la Cour de cassation).

Ces dispositions sont globalement conformes à la Convention 108 et son Protocole additionnel (article.1.4).

Remarques supplémentaires

Il y a lieu de faire remarquer que :

- Il y a un certain nombre de définitions complémentaires, qui concernent notamment les notions de : tiers, bénéficiaire, communication, interconnexion et sous-traitant.

- Des obligations complémentaires sont prévues concernant les procédures préliminaires de traitement des données à caractère personnel (article 7) qui prévoit que « toute opération de traitement des données à caractère personnel est soumise à une déclaration préalable déposée au siège de l'Instance [...]. »

- l'article 22 prévoit des conditions supplémentaires que doit satisfaire la personne pour être responsable de traitement. Le Comité s'interroge sur l'applicabilité et les conséquences de la condition relative à la nationalité tunisienne du responsable de traitement.

- Les articles 69 à 74 régissent les traitements de données à caractère personnel à des fins de vidéo-surveillance.

Conclusion

Eu égard à ce qui précède, le T-PD estime que la législation tunisienne sur la protection des données tend de manière générale vers les principes donnant effet à la Convention 108 et à son Protocole additionnel tout en nécessitant plusieurs aménagements afin de s'y conformer complètement, aussi recommande-t-il au Comité des Ministres d'inviter la République tunisienne, après s'être conformée aux observations formulées ci-dessus, à adhérer à ces deux instruments.