COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 7 February / février

T-PD(2017)02Mos

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

(T-PD)

COMPILATION OF OPINIONS / COMPILATION DES AVIS

Directorate General of Human Rights and the Rule of Law /

Direction Générale droits de l'Homme et Etat de droit

TABLE DES MATIERES

OPINION ON THE DATA PROTECTION IMPLICATIONS OF THE PROCESSING OF PASSENGER NAME RECORDS

Table of Contents

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n°108, hereinafter referred to as 'Convention 108'),

Recalling the European Convention on Human Rights (ECHR) and in particular Articles 8 (right to respect for private life) and 13 (right to an effective remedy), as further elaborated by the jurisprudence of the European Court of Human Rights and Article 2 (freedom of movement) of Protocol No. 4,

Having regard to Convention 108 and other relevant Council of Europe instruments in the field of data protection such as Recommendation (87)15 regulating the use of personal data in the police sector and Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

Noting the rapid spread at global level of information technology systems and legislations concerning the transmission by air carriers of personal data of their passengers to public authorities for law enforcement and national security purposes,

Resolved to support respect for human rights with regard to the processing of personal data of air transport by public authorities responsible for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes,

Adopted the present opinion:

1. Introduction

The 32nd Plenary meeting (1-3 July 2015) of the Consultative Committee of Convention 108 decided, in light of the growing concerns raised by reactions to the recent terrorist attacks and threats, to prepare the present opinion, having notably considered the issues addressed in the report "Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards"[1].

The Bureau of the Committee, during its 36th (6-8 October 2015), 37th (9-11 December 2015) and 38th meetings (22-24 March 2016) worked on the preparation of the Opinion, which was examined by the 33rd Plenary meeting of the Committee of Convention 108 after written consultation of the delegations and interested stakeholders.

[1] Report prepared by Mr D. Korff with the contribution of Ms M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/TPD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

The Committee of Convention 108 understands that, in the recent context of accrued menace of terrorist attacks, the fight against terrorism must be reinforced. It underlines the importance of combating terrorism efficiently and effectively while ensuring respect for human rights, the rule of law and the common values upheld by the Council of Europe. The Committee notes the willingness of governments to establish systems allowing the screening of personal data relating to air passengers as one of the means to prevent terrorism and other serious crimes, as an element of their efforts to ensure the security of the population. In this context, the Committee considers it necessary to recall the data protection principles that are applicable to such systems, underlining that the interference with human rights, including the right to the protection of private life and to the protection of personal data can only occur when the necessary conditions have been fulfilled.

Article 8 of the ECHR and Article 9 of Convention 108 have set the conditions that must be respected when a limitation to the rights to private life and data protection is considered. Such a limitation must be in accordance with a clear law and must be necessary in a democratic society for a legitimate aim (such as national security, public safety or the prevention of crime).

2. Description of PNR data

Several types of passenger data exist and for the purposes of the present opinion, the Committee will focus on Passenger Name Records (PNRs).

PNRs are records used in the air transport industry for commercial and operational purposes in providing air transportation services. The PNRs are created by airlines and travel agencies[2], relating to travel bookings in order to enable an exchange of information between them and in accordance with the passengers' requests. Such records are captured in many ways as the reservations[3] can be created in Global Distribution Systems (GDS), Computer Reservation Systems (CRS), or the airline's own reservation system. Data fed into an airline's Departure Control System (DCS) upon check-in by the passenger (i.e. seat and baggage information) can also be added automatically to an existing PNR when the CRS and DCS are integrated in a single system.

Although PNRs were originally introduced for air travel, CRS can now also be used for bookings of hotels, car rental, boat and train trips.

The format and content of a PNR, due to the common needs of multiple actors, has been progressively harmonised and standardised by the International Air Transport Association (IATA) which provides support in the design of passenger data programs.

The PNR information is collected from passengers and contains part or whole of the following items:

- Full name[4]
- address and contact information (phone number, e-mail address, IP address)
- type of travel document, number, country of issuance and date of expiry[4]
- date and country of birth[4]
- nationality[4]
- country of residence
- travel itinerary (dates, place of departure and arrival)
- address for the first night spent in the country of destination

[2] In the future, "non-carriers economic operators" (i.e. travel agencies and tour operators) may be obliged to provide PNR data to the national competent authorities.

[3] Among traditional global distribution systems, Amadeus is the only one located in Europe, with Headquarters in Spain, its Data Centre in Germany and its Research and Development Centre in France. It is owned and used notably by Air France, Iberia Airlines, Lufthansa, British airways and Scandinavian airlines and over 60 other carriers across the globe are affiliated to it.

[4] Information verified on the basis of passport information presented by the passenger.

- method of payment used, including billing address and credit card details
- frequent flyer data and benefits (free upgrade or ticket)
- an open field with general remarks (“Special Service Request”, "Optional Services Instruction" or "Other Service Information”) such as all available information on unaccompanied minors, dietary and medical requirements, seating preferences, languages, details of disability, and other similar requests.
- an individual reference (PNR record locator code)
- information on the travel agency/travel agent
- ticket information (number, date of reservation, date of issuance, one-way tickets)
- fare details and the restrictions possibly applying to this fare (and related taxes)
- names and number of other passengers travelling together on the same PNR
- travel status of passengers, including confirmations, check-in status, ‘no show’ or ‘go show’ information;
- seat number and other seating information
- code share information
- split/divided information (where the itineraries of several passengers under a PNR are not similar and changes must be brought to the booking for one passenger of an existing PNR)
- baggage information
- historic of all changes to PNR information listed above.

In practice, the content of each existing PNR will greatly vary as the number and nature of fields to complete will depend on the itinerary (e.g. in case of round-trip itinerary covering several towns in a same country or in several countries), the offer of services by airlines and the reservation system used (over 60 fields to be completed for some of them).

The fact that the information collected is provided by passengers, or by others on their behalf and that such information is not systematically checked (to the exception for instance of flight information provided by the airlines and passport information, when passports are not forged), is also to be considered, in relation to the principle of data accuracy. There is a potential for error: a PNR may contain incorrect information about an individual, which could, in some circumstances, raise suspicion.

Airlines may have a legal obligation to transfer all or part of PNR data to the competent public authorities in order to identify persons suspected of involvement in terrorist activities or serious crimes.

3. Legality

While PNRs can be of benefit to the competent public authorities in pursuing a legitimate aim, a number of conditions have to be met in order for the interference with the rights to private life and data protection to be permissible.

Pursuant to the case-law of the European Court of Human Rights relating to Article 8 of the ECHR such interference is only permissible where it is in accordance with the law and is strictly necessary and proportionate to the legitimate aim pursued.

While the assessment of the necessity of the interference, and the proportionality of the measures considered, have to be carefully examined in light of various elements, the Committee will briefly recall what the ECHR considers to be covered by the condition of legality. The requirement that any interference be ‘in accordance with the law’ (or ‘provided for by the law’ as prescribed in Article 9 of Convention 108) will only be met when three conditions are satisfied:

- the measure must have some basis in domestic law,
- this law must be clear and precise enough to be accessible to the person concerned (it must obviously be public), and
- have foreseeable consequences (enabling the person, if need be with appropriate advice, to regulate her or his conduct and act accordingly)[5].

[5] ECHR Kennedy v. the United Kingdom, § 151; Rotaru v. Romania, 28341/95, §§50, 52 and 55; Amann v. Switzerland, § 50; Iordachi and Others v. Moldova; Kruslin v. France, § 27; Huvig v. France, § 26; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, § 71; Liberty and Others v. the United Kingdom, § 59, etc.

In the context of processing of PNRs by law enforcement authorities, the criterion of the quality of the law implies a very precise and strict definition of the legitimate aim pursued.

4. Necessity and proportionality

Any prescribed or envisaged measures on processing PNR data by the competent public authorities, in light of the interference that they may entail with the rights of the data subjects, must be subject to scrutiny of their necessity and proportionality. The Committee calls for the examination of objective elements enabling to assess such necessity, the proportionality of the measures prescribed as well as the efficiency and effectivity of the system (which should be demonstrable where such systems already exist).

The processing of PNR data – providing the unique benefit of enabling the identification of individuals of interest – is the general and indiscriminate screening of all passengers, including individuals who are not suspected of any crime, by different competent authorities and concerns data initially collected for commercial purposes by private entities. In light of the degree of interference with the rights to private life and data protection that would arise from such processing, the fact that this processing is a necessary measure in a democratic society for a legitimate aim has to be clearly evidenced and the appropriate safeguards must be put in place. A specific demonstration of the necessity is needed for the collection and further use of PNR data.

The European Court of Human Rights underlined that "while the adjective 'necessary' […] is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'."[6]

While the State has a margin of appreciation in choosing the necessary means to achieve its legitimate and necessary aim, it must assess whether the interference created by such measures corresponds to a 'pressing social need'[7]. The assessment of the proportionality of the derogation needs to be based on the examination of a wide variety of elements such as the definition of clear and limited purposes, of the scope of application of the system, of the nature of the data concerned, the nature of the processing, the modalities of access to and conservation of the data, etc.

Deciding on the validity of the Data Retention Directive (regarding the retention of communication data), the Court of Justice of the European Union underlined[8] that "the derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".

In case of existing systems of processing of PNR data by the competent public authorities, greater transparency on the assessment of the efficacy of such systems should be sought with a view to enabling a sound independent assessment of the necessity of the system. While such transparency should be detailed, it should not defeat the legitimate purpose. For instance, objective and quantifiable information regarding results achieved, such as the number of arrested persons, terrorist threats which could be avoided, other deterrent effects, the modification of criminals' behaviours (e.g. abandoning originally intended criminal acts), the likelihood of substantially increased costs and difficulty of perpetrating crimes (like terrorist attacks) would help inform an assessment as to whether a PNR system is necessary.

A regular review at periodic intervals of the necessity of the PNR system to pursue its appropriate justification in time should be carried out.

[6] Handyside v. UK, 5493/72, §48.
[7] Olsson v. Sweden, 10465/83.
[8] Digital Rights Ireland, C-293/12 of 8 April 2014, §52.

5. Application of the principles and safeguards

(a) Purpose limitation

Given the level of the interference with the rights to private life and data protection posed by the processing of PNR data by competent public authorities, the purposes need to be clearly and precisely predefined by law on the basis of objective criteria which limit the transmission of the data only to the competent authorities as well as the further use of such data.

PNR systems are generally justified on the basis of the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes (such as drug trafficking, human trafficking, child trafficking, money laundering), or international crimes (such as crimes against humanity, torture, or genocide) and a clear delimitation of those legitimate aims and corresponding notions is needed in order to strictly circumscribe the use of such systems.

The definition of 'terrorism' and 'terrorist offences' is of particular complexity (see the relevant UN Conventions, the Council of Europe Convention on the prevention of terrorism of 2005 and its 2015 additional protocol). In the absence of a clear delimitation, this terminology should be restrictively construed. Should that not be the case, the purpose of the PNR system would remain too vague and the principle of proportionality would not be respected.

In exceptional cases, the prevention of serious threats to the public (for instance for the prevention of the spread of a dangerous contagious disease) could also justify the use of PNR data.

(b) Competent authorities

In order to guarantee the proportionality of the interference with the rights of the persons concerned, the public authorities receiving the PNR data should be the authorities responsible for the previously defined legitimate purposes.

Furthermore, the establishment of dedicated coordination units (such as the 'Passengers Information Units' in the EU scheme) contributes to preventing a mix between judicial and surveillance activities but the competencies of such units need to be strictly and narrowly defined and made public.

Competent national authorities legally authorised to process PNR data should be listed and that information should be made public.

(c) Passenger's personal data

The data transmitted and further processed by the competent public authorities need to be relevant, adequate and proportionate (Article 5 of Convention 108) to the purposes for which they are processed. The transmitted data must be clearly defined (the elements of the PNR that are to be transmitted must be exhaustively listed), on the basis of objective criteria, and limits to the subsequent use of such data must also be established.

PNRs contain information that is needed to facilitate a passenger's travel, and may include a number of sensitive data which could serve to indicate racial origin, political opinions or religious or other beliefs or data relating to a person's health or sexual orientation, not only under certain 'coded' data but also under the open field containing general remarks (such as dietary or medical requirements, or the fact that a political or religious association benefited from reduced fares for the travel of its members) which could lead to direct discrimination.

While the competent authorities receiving such data in the PNRs can be allowed to process it in exceptional and strictly justified circumstances (no assessment can be run on the basis of a criteria linked to any sensitive data), the Committee considers that a prohibition of the systematic use by the competent public authorities of such sensitive data should be established as a principle.

(d) Data transmission

Two different methods of transmission of the data from the commercial sector to the competent authorities of the public sector exist:

- the 'pull' method whereby public authorities directly reach into ('access') the reservation system and extract ('pull') a copy of the required data from it;
- the 'push' method whereby the operator transmits ('pushes') the required PNR data into the database of the authority requesting them.

The Committee considers that the 'push' method, with the operator being fully responsible for the quality of the data and the conditions of transmission, is to be preferred as it offers greater data protection safeguards than the 'pull' one.

(e) Data matching and mining

The processing of personal data may concern all passengers and not only the targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order.

The PNR data may be compared ('data matching') to databases[9] (i.e. of convicted persons for serious crimes, of persons under investigation for suspicion of terrorist activities, of lost and stolen passports) held by the competent authorities according to the law, in order to identify suspects or offenders as well as the persons linked to such potential suspects or offenders ('contact chaining').

PNR data may also be processed with the intention of identifying anyone who 'might' be involved in, or who 'might become' involved in criminal activities defined by the law establishing the sharing of PNRs with the competent authorities e.g. individuals travelling to become foreign terrorist fighters. This may be achieved by 'data mining' according to selectors or according to predictive algorithms.

This assessment of passengers by data mining may raise the question of predictability, in particular when operated on the basis of predictive algorithms using dynamic criteria which may constantly evolve in light of self-learning capacities.

The development of data mining algorithms should be based on the results of regular assessments of the likely impact of the data processing on the rights and fundamental freedoms of data subjects.

The basic structure of the analyses should be based on predefined risk indicators which have been clearly identified in advance.

The relevance of individual results of such automatic assessments should be carefully examined on a case-by-case basis, by a person in a non-automated manner.

(f) Conservation of data

[9] Databases created, operated and kept up-to date according to the law.

The period of retention of the PNR data must be clearly specified and limited to the time absolutely necessary for the purpose prescribed as it must be "based on objective criteria in order to ensure that it is limited to what is strictly necessary"[10]. Such criteria should be made publicly available.

Masking out[11] some elements of the data which identify the passenger, after a pre-determined period of time, which is as short as possible, can mitigate the risks entailed by a longer period of conservation, such as for instance abusive access, of the data on all passengers.

It should be recalled that masked out data still permits identification of the individuals and continues as such to constitute personal data, and that its conservation should also be limited in time in order to prevent a permanent and general surveillance.

(g) Rights of information, access, rectification and deletion

The Committee recalls that according to Article 1 of both the ECHR and Convention 108, the rights to privacy and data protection have to be secured for every individual within the jurisdiction of the contracting Parties, irrespective of her or his nationality or residence.

The person whose PNR data is being transmitted to the competent authorities is entitled to know what processing is done by such authorities (nature of the data, for which purpose and how, for how long), has a right of access and to ask for rectification or deletion of personal data.

While such rights can be limited under the restrictive conditions previously mentioned (where it is in accordance with the law and necessary in the interest of a legitimate aim), the Committee recommends that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of those rights. Persons who are suspected of having committed, or being about to commit such offences may at least request the correction of inaccurate data and the deletion of unlawful data.

Any limitation of those rights must be made known to passengers at the time of collection of their data and during the whole processing activity by the competent public authorities.

Where data concerning a passenger have been collected without her or his knowledge, and unless the data are deleted, that person should be informed, where practicable, that information is held about her or him as soon as the object of the purpose for collection is no longer likely to be prejudiced.

The persons concerned should be informed on how to exercise their rights and what remedies are available.

(h) Security

As required by Article 7 of Convention 108, appropriate security measures shall be taken for the protection of personal data. This notably implies that the PNR system shall be held in a secure physical environment, with high-level intrusion controls and a strict access (to a limited number of persons) control (such as layered logins and the production of an audit record of access). Furthermore, communication of the PNR data to the competent authorities must be protected by technical and procedural means (e.g. strong cryptography, effective procedures for managing keys, etc).

(i) Transborder Data flows

[10] Digital Rights Ireland, C-293/12 of 8 April 2014 §64.
[11] 'Masking out' means rendering invisible certain data elements enabling to identify a person.

The Committee recalls that any PNR data transfers to States that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects in such States.

(j) Remedies

It is an essential requirement of the case law of the European Court of Human Rights that "effective remedies" against violations of fundamental rights exist and be available to individuals (and not solely to nationals of the particular country concerned). While the Court of Justice of the European Union expressly mentions the requirement for redress before a tribunal, the European Court of Human Rights ruled[12] that the absence of judicial control does not necessarily constitute a violation of the rights at stake as long as other strong safeguards are provided for by the legislation (for instance independent oversight by authorities vested with sufficient powers and competence to exercise an effective and continuous control).

Article 10 of Convention 108 requires that Parties "establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection" set out in the Convention.

The Committee supports the need to provide for effective redress to the individual, which would cover both administrative and judicial remedy. The Committee also highlights the importance, as a pre-condition to an effective remedy, for the person concerned to be fully informed regarding the processing of her or his personal data and underlines the difficulties which exist in providing effective remedies against algorithm-based decisions and challenging inferences based on data analysis (false positives and other discriminatory measures).

(k) Oversight and transparency

It is clear from the case law of the European Court of Human Rights that the oversight of the authorities responsible for surveillance should be performed by an independent and external body.

The Committee underlines the role of the competent data protection authorities, which should not only be consulted in the normative process of adoption of the related laws and regulations but could also assess the compliance of a PNR system with data protection rules on the basis of individual complaints that they could receive, or on their own initiative.

Other specialised independent authorities (such as a parliamentary commission) in charge of overseeing law enforcement and intelligence agencies can also have a role in controlling the scope of application of the system, its efficiency and perform case-by-case controls regarding the rationale of the retention of the passenger's data and the duration of this retention.

Supervision by independent data protection authorities, by specialised independent authorities in charge of overseeing law enforcement and intelligence agencies, as well as through independent assessments of the efficiency by the competent authorities themselves could lead to greater transparency and accountability of the powers and competencies of a PNR system.

In addition, dedicated data protection officers should be designated within the competent authorities processing PNR data with a view to ensuring compliance and accountability of the system (with a regular evaluation of the risks at stake and systematic audits of the PNR), the data processing and communication of the data, its updating and deletion, as well as the information provided to passengers. Data protection officers could also have a role as contact points in case of complaints or requests by the persons concerned. They are encouraged to raise awareness on "good practices".

[12] Klass and Others v. Germany, §§ 55-56; Kennedy v. the United Kingdom, § 167.

6. Conclusions

In view of the special interference with the rights to data protection and privacy that PNR measures may represent, the legality, proportionality and necessity of a PNR system need to be strictly respected and demonstrated, thus implying notably the following:

- transparent demonstration in a measurable form of the necessity and proportionality of the system in light of the legitimate aim pursued;

- accurate and strict definitions of the legitimate aim pursued are required and processing of PNR data is only allowed for the defined limited grounds (prevention, detection, investigation and prosecution of terrorist offences and other serious crimes, or in exceptional cases, prevention of serious threats to the public);

- publicity of the competent public authorities (ideally dedicated coordination units);

- transmission of data via 'push method' with a clear definition of the initial retention period and appropriate security measures;

- prohibition of the systematic use of sensitive data;

- limitation of the data mining to predefined risk indicators , with case-by-case examination of the relevance of the results in a non-automatic manner;

- legal and only necessary limitations to the rights of information, access, rectification and deletion of the individuals;

- competence of the data protection authorities (to be consulted and able to assess the PNR system as well as to deal with individual complaints);

- availability of effective administrative and judicial remedies for the individuals;

- independent and external oversight of the PNR system;

- periodic review of the PNR systems by the competent authorities.

AVIS SUR LES IMPLICATIONS EN MATIERE DE PROTECTION DES DONNEES DU TRAITEMENT DES DOSSIERS PASSAGERS

Table des matières

Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108, ci-après la « Convention 108 »),

Rappelant la Convention européenne des droits de l'homme (CEDH), en particulier ses articles 8 (droit au respect de la vie privée) et 13 (droit à un recours effectif), tels que développés plus avant par la jurisprudence de la Cour européenne des droits de l'homme, et l'article 2 (liberté de circulation) du Protocole n° 4,

Considérant la Convention 108 et les autres instruments pertinents du Conseil de l'Europe dans le domaine de la protection des données, notamment la Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police et la Recommandation (2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage,

Notant l'expansion rapide, au niveau mondial, des systèmes informatiques et des législations ayant trait à la transmission par les transporteurs aériens des données à caractère personnel de leurs passagers aux autorités publiques pour assurer le respect de la loi, le maintien de l'ordre et la sécurité nationale,

Résolu à promouvoir le respect des droits de l'homme dans le contexte du traitement des données à caractère personnel des passagers aériens par les autorités publiques en charge de la prévention, de la détection, de l'instruction et de la poursuite des infractions de terrorisme et autres infractions pénales graves,

Adopte le présent avis :

1. Introduction

Face aux préoccupations grandissantes que suscitent les réactions aux récents attentats et menaces terroristes, il a été décidé, lors de la 32e réunion plénière (1-3 juillet 2015) du Comité consultatif de la Convention 108, de préparer le présent avis, en tenant notamment compte des aspects traités dans le rapport intitulé « Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards » (Dossiers passagers (PNR), exploration et protection des données : nécessité de garanties solides – en anglais uniquement)[13].

Lors de ses 36ème (6-8 octobre 2015), 37ème (9-11 décembre 2015) et 38ème (22-24 mars 2016) réunions, le Bureau du Comité s'est employé à préparer l'avis, qui a été examiné à la 33e réunion plénière du Comité de la Convention 108 après consultation écrite des délégations et des parties intéressées.

Le Comité de la Convention 108 reconnaît que, dans le contexte récent de l'intensification des menaces d'attentats terroristes, la lutte contre le terrorisme doit être renforcée. Il souligne qu'il est important de le combattre de façon efficace et effective tout en veillant au respect des droits de l'homme, de l'état de droit et

[13] Rapport préparé par M. D. Korff avec la contribution de Mme M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/TPD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

des valeurs communes défendues par le Conseil de l'Europe. Le Comité prend note de la volonté des gouvernements de mettre en place, au nombre des moyens de prévention du terrorisme et autres infractions pénales graves et dans le cadre des efforts qu'ils déploient pour garantir la sécurité de la population, des systèmes de filtrage des données à caractère personnel relatives aux passagers aériens. Dans ce contexte, le Comité juge nécessaire de rappeler les principes de protection des données applicables à ces systèmes, en soulignant qu'une atteinte aux droits fondamentaux, et notamment à la protection de la vie privée et à la protection des données à caractère personnel, n'est acceptable que sous certaines conditions impératives.

L'article 8 de la CEDH et l'article 9 de la Convention 108 ont fixé les conditions qui doivent être respectées lorsqu'est envisagée une restriction des droits au respect de la vie privée et à la protection des données. Cette restriction doit être conforme à une loi clairement formulée ; elle doit en outre être nécessaire, dans une société démocratique, à la poursuite d'un but légitime (comme la sécurité nationale, la sûreté publique ou la prévention des infractions pénales).

2. Description des données PNR

Il existe plusieurs types de données relatives aux passagers ; aux fins du présent avis, le Comité concentrera son attention sur les dossiers passagers (PNR).

Les PNR sont des dossiers utilisés par les exploitants aériens aux fins commerciales et opérationnelles de la fourniture de services de transport aérien. Les PNR sont créés par les compagnies aériennes et les agences de voyages[14], en relation avec les réservations de voyage, afin de permettre un échange d'informations entre elles et en conformité avec les demandes des passagers. Ces dossiers sont saisis de plusieurs façons, étant donné[15] que les réservations peuvent être créées dans des systèmes mondiaux de distribution (GDS pour « Global Distribution Systems »), des systèmes informatisés de réservation (SIR) ou le système de réservation propre à la compagnie aérienne. Les données saisies dans le système de contrôle des départs (DCS pour « Departure Control System ») de la compagnie aérienne au moment de l'enregistrement du passager (c'est-à-dire, le numéro de siège et les informations relatives aux bagages) peuvent également être ajoutées automatiquement à un PNR existant lorsque le SIR et le DCS sont intégrés dans un même système.

Bien que les PNR aient été institués à l'origine pour le transport aérien, le SIR peut dorénavant aussi être utilisé pour les réservations d'hôtel, les locations de voiture ou les déplacements en bateau ou en train.

Compte tenu des besoins communs de multiples acteurs, le format et le contenu des PNR ont été progressivement harmonisés et normalisés par l'Association internationale du transport aérien (IATA), qui apporte son aide dans la conception de programmes relatifs aux données passagers.

Un PNR contient tout ou partie des informations suivantes fournies par les passagers :

- nom complet[16] ;
- adresse et autres coordonnées (numéro de téléphone, adresse électronique, adresse IP) ;
- type de document d'identité, numéro, pays de délivrance et date d'expiration[17] ;
- date et pays de naissance[18] ;
- nationalité[19] ;
- pays de résidence ;
- itinéraire (dates, lieu de départ et d'arrivée) ;
- adresse pour la première nuit passée dans le pays de destination ;

[14] A l'avenir, les « opérateurs économiques non transporteurs » (c'est-à-dire les agences de voyages et les tour-opérateurs) pourraient être tenus de communiquer les données PNR aux autorités nationales compétentes.

[15] Parmi les systèmes mondiaux de distribution traditionnels, Amadeus est le seul établi en Europe (siège en Espagne, centre de données en Allemagne et centre de recherche-développement en France). Il appartient notamment à Air France, Iberia, Lufthansa, British Airways et Scandinavian Airlines, qui l'utilisent ; plus de 60 autres transporteurs dans le monde y sont affiliés.

[16] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.
[17] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.
[18] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.
[19] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.

- méthode de paiement utilisée, avec adresse de facturation et informations sur la carte de crédit ;
- profil de client fidèle et avantages (billet gratuit ou surclassement sans frais) ;
- un champ ouvert avec des observations générales (« Demande de prestations spéciales », « Instructions relatives aux services optionnels » ou « Informations sur les autres services »), telles que l'ensemble des informations disponibles sur les mineurs non accompagnés, les demandes diététiques et médicales, les préférences de siège, les langues, les renseignements concernant un handicap et autres demandes similaires ;
- référence individuelle (code du dossier PNR) ;
- informations sur l'agence de voyage ou l'agent de voyage ;
- données du billet (numéro, date de réservation, date d'émission, aller simple) ;
- détail du prix et restrictions éventuellement applicables au tarif (et taxes) ;
- noms et nombre de passagers voyageant ensemble figurant dans le même PNR ;
- statut des passagers (confirmations, enregistrement, non-présentation ou passager de dernière minute sans réservation) ;
- numéro du siège et autres informations concernant le siège ;
- partage de code ;
- information scindée/divisée (lorsque les itinéraires de plusieurs passagers d'un PNR ne sont pas identiques et que des modifications doivent être apportées à la réservation d'un passager d'un PNR existant) ;
- bagages ;
- historique de toutes les modifications des données PNR susmentionnées.

Dans la pratique, le contenu des PNR varie sensiblement d'un cas à l'autre, étant donné que le nombre et le type des champs à compléter dépendent de l'itinéraire (par exemple, dans le cas d'un aller-retour couvrant plusieurs villes dans un même pays ou dans plusieurs pays), de l'offre de services des compagnies aériennes et du système de réservation utilisé (plus de 60 champs à renseigner dans certains cas).

Le fait que les informations recueillies soient fournies par les passagers, ou pour leur compte, et qu'elles ne soient pas systématiquement vérifiées (à l'exception par exemple des informations relatives au vol fournies par les compagnies aériennes et des informations figurant sur le passeport, lorsque celui-ci n'est pas un faux) doit aussi être pris en compte en relation avec le principe d'exactitude des données. Il existe un risque d'erreur puisqu'un PNR peut contenir des informations incorrectes sur une personne, qui pourraient, dans certaines circonstances, éveiller les soupçons.

Les compagnies aériennes peuvent avoir l'obligation légale de transférer tout ou partie des données PNR aux autorités publiques compétentes afin d'identifier des personnes soupçonnées de participation à des activités terroristes ou autres crimes graves.

2. Légalité

Si les PNR peuvent présenter un intérêt pour les autorités publiques compétentes dans la poursuite d'un but légitime, il faut qu'un certain nombre de conditions soient remplies pour que l'atteinte aux droits à la vie privée et à la protection des données qu'ils représentent puisse être permise.

Selon la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la CEDH, une telle atteinte n'est permise que si elle est prévue par la loi et strictement nécessaire et proportionnée au but légitime visé.

Si la nécessité de l'atteinte et la proportionnalité des mesures envisagées doivent faire l'objet d'un examen approfondi en tenant compte de divers éléments, le Comité rappelle brièvement ce que recouvre, d'après la CEDH, la condition de légalité. L'exigence que toute atteinte soit « conforme à la loi » (ou « prévue par la loi » aux termes de l'article 9 de la Convention 108) implique que trois conditions soient remplies :

- la mesure doit être fondée en droit interne,
- la loi doit être suffisamment claire et précise pour être accessible à la personne concernée (elle doit à l'évidence être rendue publique), et

- la loi doit avoir des conséquences prévisibles (permettant à la personne, au besoin à l'aide de conseils appropriés, de régler son comportement et d'agir en conséquence)[20].

Dans le contexte du traitement des PNR par les services chargés du respect de la loi, le critère de la qualité de la loi implique une définition très précise et rigoureuse du but légitime visé.

3. Nécessité et proportionnalité

Vu l'atteinte aux droits des personnes concernées qui peut découler des mesures prescrites ou envisagées concernant le traitement des données PNR par les autorités publiques compétentes, il est indispensable de démontrer la nécessité et la proportionnalité de ces mesures. Le Comité demande l'examen des éléments objectifs qui permettent d'évaluer cette nécessité, la proportionnalité des mesures prescrites, ainsi que l'efficacité et l'effectivité du système (qui doivent pouvoir être démontrées lorsque de tels systèmes existent déjà).

Le traitement des données PNR – qui a l'avantage unique de permettre l'identification des personnes d' intérêt - est un filtrage général et non sélectif de tous les passagers, y compris de ceux qui ne sont pas soupçonnés d'avoir commis une quelconque infraction pénale, par différentes autorités compétentes, et il concerne des données collectées initialement à des fins commerciales par des entités privées. Eu égard à l'ampleur de l'atteinte aux droits à la vie privée et à la protection des données qui découlerait du traitement des données PNR, il doit être clairement établi que ledit traitement est une mesure nécessaire dans une société démocratique dans un but légitime ; il faut en outre que les garanties appropriées soient mises en place. Il est indispensable de démontrer expressément la nécessité de la collecte et de l'exploitation ultérieure des données PNR.

La Cour européenne des droits de l'homme a souligné que « si l'adjectif "nécessaire" (…) n'est pas synonyme d'"indispensable" (…), il n'a pas non plus la souplesse de termes tels qu'"admissible", "normal" (…),"utile" (…),"raisonnable" (…) ou "opportun" »[21].

Disposant d'une marge d'appréciation dans le choix des moyens nécessaires pour atteindre son but légitime et nécessaire, l'Etat doit déterminer si les atteintes induites par ces mesures correspondent à un « besoin social impérieux »[22]. L'évaluation de la proportionnalité de la dérogation doit reposer sur l'examen d'un vaste ensemble d'éléments tels que la définition de buts clairs et limités, du champ d'application du système, de la nature des données concernées, de la nature du traitement, des modalités d'accès aux données et de leur conservation, etc.

Se prononçant sur la validité de la directive sur la conservation des données (en ce qui concerne la conservation des données de communication), la Cour de justice de l'Union européenne a souligné[23] que « les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire ».

Dans le cas des systèmes existants de traitement des données PNR par les autorités publiques compétentes, une plus grande transparence sur l'évaluation de l'efficacité de ces systèmes doit être recherchée en vue de permettre une évaluation fondée et indépendante de la nécessité du système. Si cette transparence doit être détaillée, elle ne doit toutefois pas aller à l'encontre de l'objectif légitime. Par exemple, des informations objectives et quantifiables concernant les résultats atteints, comme le nombre de personnes arrêtées, les menaces terroristes qui pourraient être évitées, les autres effets dissuasifs, la modification des comportements des délinquants (par exemple, le renoncement à des actes criminels envisagés), la probabilité d'une augmentation importante du coût et de la difficulté de la perpétration d'infractions (tels que des attentats terroristes) permettraient d'éclairer l'évaluation de la nécessité d'un système de traitement des PNR.

[20] Cour européenne des droits de l'homme : *Kennedy c. Royaume-Uni*, § 151 ; *Rotaru c. Roumanie*, 28341/95, §§ 50, 52 et 55 ; *Amann c. Suisse*, § 50 ; *Iordachi et autres c. Moldova* ; *Kruslin c. France*, § 27 ; *Huvig c. France*, § 26 ; *Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev c. Bulgarie*, § 71 ; *Liberty et autres c. Royaume-Uni*, § 59 ; etc.
[21] *Handyside c. Royaume-Uni*, 5493/72, §48.
[22] *Olsson c. Suède*, 10465/83.
[23] *Digital Rights Ireland*, C 293/12 du 8 avril 2014, § 52.

Il convient de procéder à intervalles réguliers à un examen de la nécessité du système des PNR afin de déterminer s'il est toujours justifié.

4. Application des principes et garanties

(l) Limitation des finalités

Eu égard au degré d' atteinte aux droits à la vie privée et à la protection des données, induites par le traitement des données PNR par des autorités publiques compétentes, les buts doivent être définis par la loi de façon claire et précise sur la base de critères objectifs qui limitent la transmission de ces données uniquement aux autorités compétentes ainsi que le traitement ultérieur de ces données.

Les systèmes des PNR étant généralement justifiés par la prévention, la détection, l'instruction et la poursuite des infractions de terrorisme et autres infractions pénales graves (comme le trafic de drogues, la traite des êtres humains, la traite d'enfants, le blanchiment de capitaux) ou des crimes internationaux (comme les crimes contre l'humanité, les actes de torture ou le génocide), une délimitation claire de ces buts légitimes et notions correspondantes est nécessaire afin de circonscrire rigoureusement l'utilisation de ces systèmes.

La définition des termes « terrorisme » et « actes de terrorisme » est particulièrement complexe (voir les conventions pertinentes des Nations Unies, la Convention du Conseil de l'Europe pour la prévention du terrorisme de 2005 et son Protocole additionnel de 2015) ; en l'absence d'une délimitation claire, ces termes doivent être interprétés de façon restrictive. Dans le cas contraire, la finalité du système de PNR resterait trop vague et le principe de proportionnalité ne serait pas respecté.

Dans des cas exceptionnels, la prévention de menaces graves au public (par exemple, pour la prévention de la propagation d'une maladie contagieuse dangereuse) pourrait aussi justifier l'utilisation des données PNR.

(m) Autorités compétentes

Afin de garantir le caractère proportionné des atteintes aux droits des personnes concernées, les autorités publiques recevant les données PNR doivent être les autorités responsables des buts légitimes précédemment définis.

Par ailleurs, l'établissement d'une unité de coordination spéciale (telle que l'« unité de renseignements passagers » dans le dispositif de l'UE) peut contribuer à empêcher une superposition entre les activités judiciaires et les activités de surveillance, mais les compétences d'une telle unité doivent être définies de façon rigoureuse et restrictive et rendues publiques.

La liste des autorités nationales compétentes qui sont habilitées par la loi à traiter les données PNR devrait être dressée et cette information devrait être rendue publique.

(n) Données personnelles des passagers

Les données transmises aux autorités publiques compétentes et traitées par ces dernières doivent être pertinentes, adéquates et proportionnées (article 5 de la Convention 108) par rapport aux finalités pour lesquelles elles sont traitées. Les données transmises doivent être clairement définies (la liste complète des éléments du PNR qui doivent être transmis doit être dressée), sur la base de critères objectifs, et des limites à leur utilisation ultérieure doivent aussi être établies.

Les PNR contiennent des informations visant à faciliter le voyage d'un passager, et peuvent comprendre un certain nombre de données sensibles (données pouvant servir à indiquer l'origine raciale, les opinions politiques, les convictions religieuses ou autres, l'état de santé ou l'orientation sexuelle d'une personne), non seulement sous certaines données «codées » mais aussi dans le champ ouvert contenant des observations générales (telles que les demandes diététiques et médicales, ou le fait qu'une association politique ou religieuse a bénéficié de billets à prix réduit pour le voyage de ses membres), ce qui pourrait conduire à une discrimination directe.

Même si les autorités compétentes recevant de telles données dans les PNR peuvent être autorisées à les traiter dans des circonstances exceptionnelles et rigoureusement justifiées (aucune évaluation ne peut être

pratiquée sur la base de critères liés à des données sensibles, le Comité considère qu'une interdiction de l'utilisation systématique de telles données sensibles par les autorités publiques compétentes devrait être établie en tant que principe.

(o) Transmission des données

Il existe deux méthodes différentes de transmission des données, du secteur commercial aux autorités compétentes du secteur public :

- le mode « *pull* », par lequel les autorités publiques obtiennent un accès direct au système de réservation et en extraient une copie des données requises ;
- le mode « *push* », par lequel l'opérateur transfère les données PNR requises dans la base de données de l'autorité qui en fait la demande.

Le Comité considère que le mode « push », dans lequel l'opérateur assume l'entière responsabilité de la qualité des données et des conditions de transmission, doit être préféré, vu qu'il offre de plus grandes garanties de protection des données par rapport au mode « pull ».

(p) Mise en correspondance et exploration de données

Le traitement des données à caractère personnel peut concerner tous les passagers et pas seulement les individus ciblés soupçonnés d'être impliqués dans une infraction pénale ou de constituer une menace immédiate à la sécurité nationale ou à l'ordre public.

Les données PNR peuvent être comparées (« data matching ») à des bases de données[24] (à savoir, des bases sur les personnes condamnées pour infractions pénales graves, les personnes visées par une enquête pour soupçon d'activités terroristes, les passeports volés ou perdus) tenues par les autorités compétentes conformément à la loi afin d'identifier les suspects ou auteurs d'infractions ainsi que les personnes liées à ces suspects ou auteurs d'infractions potentiels (« graphe social »).

Les données PNR peuvent aussi être traitées dans le but d'identifier (par « data mining ») quiconque « pourrait » être impliqué ou s'engager dans les activités criminelles définies par la loi qui établit le partage des PNR avec les autorités compétentes comme, par exemple, les individus voyageant dans le but de devenir des combattants terroristes étrangers. Cela pourrait être obtenu par l'exploration de données selon des sélecteurs ou des algorithmes prédictifs.

L'évaluation des passagers par la mise en correspondance de données peut soulever la question de la prévisibilité, en particulier lorsqu'elle est effectuée sur la base d'algorithmes prédictifs utilisant des critères dynamiques susceptibles d'évoluer en permanence selon les capacités d'auto-apprentissage.

Le développement d'algorithmes d'exploration de données devrait se fonder sur les résultats d'évaluations régulières de l'impact probable du traitement de données sur les droits et libertés fondamentales des personnes concernées.

La structure de base des analyses devrait se fonder sur des indicateurs de risque prédéfinis ayant été clairement établis au préalable.

La pertinence des résultats individuels de ces évaluations automatiques devrait être examinée avec soin au cas par cas, par une personne et de façon non automatisée.

(q) Conservation des données

La durée de conservation des données PNR doit être clairement précisée et limitée au temps absolument nécessaire pour l'objectif prescrit dans la mesure où « la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire »[25]. Ces critères devraient être accessibles au public.

[24] Des bases de données créées, gérées et actualisées conformément à la loi.
[25] Digital Rights Ireland, C--293/12 du 8 avril 2014, § 64.

Masquer[26] certains éléments des données qui identifient le passager après une période prédéterminée, réduite au minimum, peut atténuer les risques induits par une période de conservation prolongée des données, comme par exemple un accès abusif, pour tous les passagers.

Il convient de rappeler que des données masquées permettent encore d'identifier les personnes et restent à ce titre des données à caractère personnel, et que leur conservation devrait aussi être limitée dans le temps pour prévenir une surveillance permanente généralisée.

(r) Droits d'information, d'accès, de rectification et d'effacement

Le Comité rappelle qu'aux termes de l'article 1 de la CEDH et de l'article 1 de la Convention 108, les droits à la vie privée et à la protection des données doivent être garantis à chaque personne relevant de la juridiction des parties contractantes, quels que soient sa nationalité ou son lieu de résidence.

La personne dont les données PNR sont transmises aux autorités compétentes a le droit de savoir comment elles sont traitées par ces autorités (nature des données, à quelles fins et comment, pour quelle durée), a un droit d'accès et a le droit de demander la rectification ou l'effacement des données à caractère personnel.

Même si la limitation de ces droits est soumise à des conditions restrictives mentionnées précédemment (à savoir que la limitation soit conforme à la loi et nécessaire pour atteindre un but légitime), le Comité recommande que les personnes qui ne sont pas soupçonnées d'avoir commis, ou d'envisager de commettre, un acte de terrorisme ou une autre infraction pénale grave jouissent du plein exercice des droits en question et que les personnes qui sont soupçonnées d'avoir commis, ou d'envisager de commettre, une telle infraction puissent au moins demander la correction de données inexactes et l'effacement de données illicites.

Toute limitation des droits considérés doit être portée à la connaissance des passagers au moment de la collecte de leurs données et pendant toute l'activité de traitement par les autorités publiques compétentes.

Lorsque des données relatives à un passager ont été recueillies à son insu, à moins qu'elles ne soient supprimées, la personne devrait être informée, si possible, que des informations sont conservées à son sujet dès que cela ne risque plus de desservir le but recherché par la collecte.

Les personnes concernées devraient être informées des modalités d'exercice de leurs droits et des voies de recours dont elles disposent.

(s) Sécurité

En application de l'article 7 de la Convention 108, des mesures de sécurité appropriées doivent être prises pour assurer la protection des données à caractère personnel. Cela suppose notamment que le système de PNR soit détenu dans un environnement physique sûr, doté de systèmes perfectionnés de protection contre l'intrusion et soumis à un strict contrôle d'accès (accès accordé à un nombre limité de personnes et basé, par exemple, sur une identification à niveaux multiples et la production d'un état d'audit des accès). En outre, la communication des données PNR aux autorités compétentes doit être protégée par des moyens techniques et procéduraux (par exemple, solide dispositif de cryptographie, procédures efficaces de gestion de clés, etc.).

(t) Flux transfrontières de données

Le Comité rappelle que tout transfert de données PNR aux Etats qui ne sont pas parties à la Convention 108 doit satisfaire aux conditions établies pour garantir la protection appropriée des personnes concernées dans ces Etats.

[26] « Masquer » signifie rendre invisibles certains éléments de données permettant d'identifier une personne.

(u) Recours

Aux termes de la jurisprudence de la Cour européenne des droits de l'homme, il est essentiel que des « recours effectifs » contre les violations des droits fondamentaux existent et soient accessibles aux individus (et pas seulement aux ressortissants du pays particulier concerné). Si la Cour de justice de l'Union européenne mentionne expressément l'obligation de recours devant un tribunal, la Cour européenne des droits de l'homme a estimé[27] que l'absence de contrôle juridictionnel ne constituait pas nécessairement une violation des droits en jeu dès lors que la législation prévoit d'autres garanties fortes (par exemple, un contrôle indépendant par des autorités disposant de pouvoirs et de compétences suffisants pour exercer un contrôle effectif et continu).

L'article 10 de la Convention 108 impose aux parties d'établir « des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données » énoncés dans la Convention.

Le Comité soutient la nécessité de prévoir une réparation effective pour les individus, qui couvrirait à la fois les recours judiciaires et administratifs. Le Comité souligne aussi qu'il est important, comme condition préalable à un recours effectif, que la personne concernée soit pleinement informée du traitement de ses données à caractère personnel, et insiste sur la difficulté de garantir un recours effectif contre des décisions fondées sur des algorithmes et de contester des atteintes fondées sur une analyse de données (faux positifs et autres mesures discriminatoires).

(v) Contrôle et transparence

Il ressort clairement de la jurisprudence de la Cour européenne des droits de l'homme que le contrôle des autorités chargées de la surveillance devrait être assuré par un organe externe indépendant.

Le Comité souligne le rôle des autorités compétentes chargées de la protection des données, qui doivent non seulement être consultées dans le cadre du processus normatif de l'adoption des lois et règlements pertinents, mais pourraient aussi évaluer la conformité d'un système de PNR avec les règles de protection des données sur la base des plaintes individuelles dont elles pourraient être saisies ou à leur propre initiative.

D'autres autorités indépendantes spécialisées (telles qu'une commission parlementaire) habilitées à surveiller les organes d'application de la loi et de renseignement peuvent également jouer un rôle s'agissant de contrôler le champ d'application et l'efficacité du système et d'effectuer des contrôles, au cas par cas, du bien-fondé de la conservation des données des passagers et de la durée de cette conservation.

Un contrôle assuré par des autorités indépendantes chargées de la protection des données et d'autorités indépendantes spécialisées chargées de surveiller les organes d'application de la loi et de renseignement ainsi que des évaluations indépendantes de l'efficacité mises en œuvre par les autorités compétentes elles-mêmes peuvent contribuer à une meilleure transparence des pouvoirs et des compétences d'un système de PNR et à une plus grande responsabilisation.

En outre, il conviendrait de nommer des délégués à la protection des données au sein des instances chargées du traitement des données PNR, pour contrôler la conformité et la transparence du système (avec une évaluation régulière des risques en jeu et un audit systématique des PNR), le traitement et la communication des données, la mise à jour et la suppression des données, ainsi que les informations communiquées aux passagers. Les délégués à la protection des données pourraient également servir d'interlocuteurs en cas de plaintes ou autres demandes des personnes concernées. Ils sont encouragés à sensibiliser aux « bonnes pratiques ».

5. Conclusions

Compte tenu de l'atteinte particulière aux droits à la protection des données et à la vie privée que les mesures PNR peuvent représenter, la légalité, la proportionnalité et la nécessité d'un système PNR doivent être strictement respectées et démontrées, ce qui suppose notamment ce qui suit :

[27] Klass et autres c. Allemagne, §§ 55 et 56 ; Kennedy c. Royaume-Uni, § 167.

- une démonstration transparente et mesurable de la nécessité et de la proportionnalité du système au regard du but légitime poursuivi ;

- des définitions précises et strictes de l'objectif légitime poursuivi sont nécessaires et le traitement des données PNR ne doit être autorisé que pour des motifs limités et bien définis (prévention, détection, instruction et poursuite des infractions de terrorisme et autres infractions graves, ou dans des cas exceptionnels, prévention de menaces graves au public) ;

- une liste publique des autorités publiques compétentes (dans l'idéal, des unités de coordination spéciales) ;

- l'utilisation du « mode push » pour transmettre des données ainsi qu'une définition claire de la période de conservation initiale et des mesures de sécurité appropriées ;

- une interdiction de l'utilisation systématique des données sensibles ;

- une exploration des données limitée par des indicateurs de risque prédéfinis, avec un examen au cas par cas de la pertinence des résultats d'une manière non automatique ;

- des limitations uniquement nécessaires et prévues par la loi aux droits d'information, d'accès, de rectification et d'effacement dont jouissent les individus ;

- la compétence des autorités chargées de la protection des données (pouvant être consultées et habilitées à évaluer le système PNR et à traiter les plaintes individuelles) ;

- la disponibilité de voies de recours administratives et judiciaires effectives pour les personnes concernées ;

- un contrôle externe indépendant du système PNR ;

- un examen régulier du système PNR par les autorités compétentes.

OPINION ON THE REQUEST FOR ACCESSION BY BURKINA FASO

Introduction

On 17 November 2016, the Secretary General of the Council of Europe received a letter dated 4 October 2016 informing him of Burkina Faso's wish 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 recalled that in 2008 it brought attention of the Committee of Ministers to its recommendation to invite non-member states with data protection legislation in compliance with Convention 108 to accede to the 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[28] Law No. 010-2004 / AN on the protection of personal data (hereinafter "the Law"[29]) and taken note of the constitution of Burkina Faso, in particular Article 6 guaranteeing the right to respect for private life, the Committee notes the following:

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

The purpose of the Law is set out in Article 1, namely *"to protect, within Burkina Faso, the rights of all individuals in connection with the processing of personal data, irrespective of the type or method of processing, or the identity of the data controller*". This statement complies with the purpose set forth in the provisions of Article 1 of Convention 108; Article 60 further states that "*with effect from the promulgation of this Law, all data processing must comply with the provisions of this Law"* and Article 62 states that *"this Law, which repeals all previous provisions stipulating otherwise, shall be implemented as a national law***".**

2. Definitions

The Law sets out the definitions of "personal data", "data processing", "controller" and "recipient" (Articles 2.a, 2.b, 2.d, 2.e of Convention 108) in Articles 2, 3, 4.1 and 4.2 respectively. The "data subject" is defined in Article 4.3 (*"the identifiable person to whom the personal data relate*").

[28] The Committee has taken note of the Supplementary Act A/SA 1/01/10 on personal data protection within the Economic Community of West African States (ECOWAS) but was not in a position to base its analysis on this Act as the corresponding publication in the official journal of Burkina Faso was not available.

[29] There is no English official translation of the Law and quotations of the Law in this document as proposed by the Secretariat for reference purposes cannot lead to any form of liability.

A. Personal data (Article 2.a of the Convention)

Article 2 of the Law defines "personal data" as "*any information which enables, either directly or indirectly, the identification of physical persons, in particular by means of a reference to an identification number or to several particular elements which are specific to their physical, psychological, mental, economic, cultural or social identity"*. This definition, which is more detailed than the one given in Convention 108, complies with the definition given in Article 2.a of the Convention.

B. Processing (Article 2.c of the Convention)

Article 3 of the Law defines "the processing of personal data" as *"any operation or set of operations performed, whether by automated processes or not, by a natural or legal person and applied to personal data, such as the collection, recording, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or interconnection, locking, erasure or destruction*". This definition corresponds to the one given in Article 2.b of Convention 108.

C. Controller (Article 2.d of the Convention)

Article 4.1 of the Law defines the "controller" as *"the natural or legal person, public or private, with the authority to decide to create personal data*". It would be helpful to expand this definition so as not to restrict classification as controller to the sole criterion of "creation", and to include the other aspects referred to in Article 2.d of Convention 108 which also makes a reference to the one who is competent "to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them".

3. Scope of the data protection regime (Article 3 of the Convention)

Article 1 of the Law states that it protects persons with regard to the processing of data "*whoever or whichever is the controller*" (that is from the public or private sector). Furthermore, Article 4.1 refers controllers in the public or private sector. Finally, Article 18 deals specifically with processing in the public sector. This scope corresponds to the scope set out in Article 3 of Convention 108 but an explicit mention of it in the Law would be welcome.

In addition, Article 8 provides that the law shall apply *"to automated or non-automated processing of personal data, contained or destined to be included in files whose controller is located on the territory of Burkina Faso or, where not located in said territory, uses processing equipment located on the territory of Burkina Faso, with the exclusion of data used solely for transit purposes*."

Furthermore, the provisions of Articles 12, 13, 15, 18, 19, 22 and 25 of the Law on the collection, recording and storage of personal data apply to non-automated or mechanised files other than those whose use concerns strictly private matters (Article 57); for these files, the criminal provisions of the Law shall also apply (Article 55).

The Committee is of the opinion that the partial exemption foreseen in Article 10 for "*data processing for the purpose of research in the health field*" (no prior information of the data subject but favourable opinion of the Authority) and the complete exemption foreseen in Article 11 of the Law for "*data processing for the purpose of individual therapeutic or medical treatment of patients*" should be re-examined so that such processing also benefit from the protection guaranteed by the provisions of the Law.

In addition, the Committee questions the articulation between the complete exemption from the scope of the Law of the "*data processing for the purpose of individual therapeutic or medical treatment of patients"* (Article 11) and the provisions of Article 17 (second paragraph) on data subjects' indirect access to medical data and the provisions of Article 20 on the prohibition of processing of sensitive data – including health data – without the consent of the data subject, except in the case foreseen in Article 21 of the Law (the last hyphen allows the data processing carried out "*for the purpose of preventive medicine, medical diagnosis and administration of treatment and of the therapy*" if carried out by persons bound by medical secrecy).

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

Articles 5, 12 and 14 contain fundamental data protection principles. The consent of the data subjects must be obtained for the processing of personal data, except where otherwise provided by law (Article 5), as in the circumstances laid down in Article 21. It should be noted that the Law does not define the criteria applicable to the 'consent'. The personal data controller must process the data in a fair, lawful and non-fraudulent manner (Article 12). The processing of data must be for "*specific, explicit and legitimate" purposes; data must be appropriate, relevant and not excessive in respect of the purposes for which they are collected and then processed; the period of storage must not exceed that necessary for the purposes for which the data are collected and processed; beyond that period, they may not be stored in nominate form except for processing for historical, statistical or research purposes"* (Article 14). The provisions of Articles 5, 12 and 14 are in conformity with those of Article 5 of Convention 108.

One could raise the issue of whether it would be better to refer to the fact that the data subject is identifiable rather than to the "nominate" form of the data stored.

Finally, the principle of the accuracy of personal data should be expressly mentioned (Article 17.3 foresees the right of the data subject to request correction or rectification of his/her personal data but the Law does not lay down the basic principle of accuracy of personal data).

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

Article 20 of the Law refers to "sensitive data", namely *"personal data relating to health … or which indicate racial or ethnic origin, political or philosophical opinions, religious beliefs, trade union membership or morals"*. Data relating to offences are specifically mentioned in Article 22. To the exception of an absence of explicit reference to 'sexual life', the special categories of data listed in the Law are in conformity with Article 6 of Convention 108.

Article 20 of the Law contains the fundamental principle of the prohibition of the processing of "sensitive data", except where provided for by law together with the appropriate safeguards. Accordingly, personal data relating to offences, convictions and security measures may be processed only by the courts and public authorities in the exercise of their lawful duties, by legal entities performing a public service, with the approval of the supervisory authority, and by officers of the court for the sole purpose of the performance of their duties (Article 22). The specific nature of the processing of personal health data is addressed in Articles 10, 11, 17.2, 17.3, 21 sixth indent, 23 (which stipulates that disclosure or commercial use of personal health data is prohibited) and 56 of the Law. In these provisions, the Law complies with Article 6 of Convention 108.

6. Data security (Article 7 of the Convention)

Article 15 of the Law provides that "*the controller must apply all appropriate technical or organisational measures to ensure the security of data and in particular protect data from accidental or unlawful destruction,*

accidental loss, alteration, dissemination or unauthorised access". This provision complies with Article 7.1 of Convention 108.

7. Additional safeguards for the data subject (Article 8.a to 8.d of the Convention)

"*The controller must inform the data subject of the purpose of the processing, the recipients of the data, the mandatory or optional nature of responding to the questions asked and any consequences of failure to respond*" (Article 13.1). The Committee welcomes the right provided for in Article 6 for any individual "*[…] to learn of and challenge the information and reasoning used in the processing, whether automated or not, the results of which are detrimental to him or her*". The provisions of the Law comply with Article 8.a of Convention 108.

Data subjects have the right to be informed of the data stored regarding them, without excessive delay or expense (Article 17.1). Regarding medical data, Article 17.2 which prescribes the systematic exercise of the right of access in an indirect manner, by the intermediary of a doctor, could be softened with a view to limiting this indirect access to certain situations only.

Article 17.3 provides for a right of rectification "*if the data are shown to be incomplete or inaccurate, the data subjects may ask for them to be rectified*". Article 16 second paragraph refers to a right of objection (*"data subjects have the right to object, on legitimate grounds, to the processing of personal data relating to them"*). The provisions of the Law comply with Articles 8.b to 8.d of Convention 108.

8. Exceptions, restrictions (Article 9 of the Convention)

The Law provides for limited exceptions and restrictions. A limitation of the rights of the data subject is set out in Article 17.4 with regard to "*processing relating to the security of the State, defence and public safety*" with indirect exercise of these rights through the intermediary of the Supervisory Authority. Moreover, the Law provides that certain provisions are not applicable to processing carried out by the press if they would result in a limitation of the exercise of freedom of expression (Article 25). The provisions of the Law comply with Article 9 of Convention 108.

9. Sanctions and remedies (Articles 8.d and 10 of the Convention)

Parts III (Article 37) and IV (Articles 46 to 54) of the Law provide for several sanctions which vary from one month to 5 years of imprisonment and from 200 000 to 500 000 CFA francs.

Furthermore the Supervisory Authority can according to Article 37.d issue warnings to concerned parties or refer to the public prosecutor the offenses it becomes aware of. Individuals can file a complaint to the Supervisory Authority (Article 37.f) or in court. In case of a negative opinion of the Supervisory Authority on a proposed data processing to be carried out for the benefit of the State, the data controller according to Article 19 can bring a dispute to the Council of State. In general all decisions of the Supervisory Authority can be appealed.

These provisions comply with Article 10 of Convention 108.

10. Transborder flows of personal data (Article 12 of the Convention and Article 2 of the Additional Protocol)

Article 24 provides that personal data which have been subject to automated processing governed by Article 19 (private sector) may be transmitted between Burkina Faso and a foreign state only where the protection

provided for by the Law is ensured, except in exceptional circumstances (notion which would need to be defined in light of the practice of the Supervisory Authority in the field) and where transmission is authorised by decree issued following the prior approval of the Supervisory Authority. The Committee recommends that the provisions of Article 24 be reconsidered in order to better regulate transborder data flows.

Regarding transborder data flows for public sector processing, Article 18 is to be applied, which also provides for the prior approval of the Supervisory Authority.

11. Supervisory Authority (Article 1 of the Additional Protocol)

The Law provides for the establishment of a Supervisory Authority, entitled "Information Technology and Freedoms Commission", referred to in Part II and Articles 10, 17.4, 18, 19, 22 second indent, 24.2, 52, 56.1 and 59 of the Law. The Commission is an independent administrative authority, whose establishment, membership, status of members, budget, large competences (*a priori* powers as well as investigative powers), publicity of data processing carried out and annual report are set out in Articles 26, 27, 28 to 34, 35 and 36, 37 to 43, 44, 45 respectively. The Commission comprises a panel of nine members appointed by the Council of Ministers, after elections or designations by their peers in different bodies or associations to which they belong, to ensure the independence of the Supervisory Authority. The members cannot be members of the government or responsible of a private company. Furthermore they swear an oath of independence and of impartiality.

These provisions comply with Article 1 of the Additional Protocol to Convention 108.

It should furthermore be noted that the Commission was established in December 2007 and can present the following outline of activity (as of 2008):

DESIGNATION	**NUMBER**
NUMBER OF STRUCTURES WHOSE FILES HAVE BEEN DEALT WITH	61 STRUCTURES
REQUESTS FOR ADVICE	50 CASES
NORMAL DECLARATIONS	144 FILES
APPROVALS OF TRANSFERS	45 FILES
REQUESTS FOR OPINION	14 FILES
COMPLAINTS	40 FORMAL COMPLAINTS HANDLED

Additional comments

The provisions of the Law do not apply to *"temporary copies made in the context of technical operations of transmission and access provision to a digital network for the purpose of automatic, intermediate and transitory retention of data and with the sole aim of allowing other recipients of the service to benefit from the best possible access to the information"* (Article 9). The Committee underlines that such an exemption is only permissible if personal data are stored for a very short period of time and if the temporary copies are deleted once the transfer is completed.

The Committee commends the provisions of Article 7: "*No court decision involving an assessment of an individual's behaviour may be based solely on the automated processing of information intended to define the profile or personality of the data subject or to assess certain aspects of his or her personality.*

No administrative or private decision involving an assessment of an individual's behaviour may be based solely on the automated processing of information intended to define the profile or personality of the data subject".

Conclusion

In the light of the above, the Committee considers that the Law on data protection of Burkina Faso, while deserving adjustments in line with the comments of this Opinion, generally *satisfies* the rules of Convention 108 and its Additional Protocol. Accordingly, the Consultative Committee, on the basis of the analysis of the applicable data protection legislation is of the opinion that the request from Burkina Faso to be invited to accede to Convention 108 and its Additional Protocol should be given a favourable response.

AVIS SUR LA DEMANDE D'ADHÉSION DU BURKINA FASO

Introduction

Le 17 novembre 2016, le Secrétaire Général du Conseil de l'Europe a reçu une lettre datée du 4 octobre 2016 lui faisant part du souhait du Burkina Faso d'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 rappelle qu'il avait en 2008 porté à l'attention du Comité des Ministres sa recommandation visant à inviter 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[30] la loi n°010-2004 / AN *portant protection des données à caractère personnel* (ci-après « la loi ») et avoir pris note de la Constitution du Burkina Faso, notamment de son article 6 garantissant le droit au respect de la vie privée, le Comité constate ce qui suit :

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

L'article 1 de la loi énonce son objet : *« protéger, au Burkina Faso, les droits des personnes en matière de traitement de données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables »*. L'énoncé correspond à la finalité des dispositions de l'article 1er de la Convention 108 et dispose par ailleurs à ses articles 60 qu'*« à compter de la promulgation de la présente loi, tous les traitements de données devront correspondre aux prescriptions de cette loi »* et 62, *« la présente loi qui abroge toutes dispositions antérieures contraires sera exécutée comme loi de l'Etat »*.

13. Définitions

La loi énonce les définitions des « données à caractère personnel », « traitement de données », « responsable du traitement » et « destinataire » (article 2.a, 2.b, 2.d, 2.e de la Convention 108) respectivement dans ses articles 2, 3, 4 alinéa 1 et 4 alinéa 2. La « personne concernée » est définie à l'article 4 alinéa 3 (*« la personne identifiable à laquelle se rapportent les données à caractère personnel »*).

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

La loi définit dans son article 2 la « donnée à caractère personnel », soit *« toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques propres à leur identité physique, psychologique, psychique, économique, culturelle ou sociale »*. Cette définition, qui est plus détaillée que celle du libellé de la Convention 108, est conforme à la définition donnée par l'article 2.a de cette dernière.

E. Traitement (article 2.c de la Convention)

[30] Le Comité a pris note de l'Acte additionnel A/SA 1/01/10 de la Communauté économique des États d'Afrique de l'Ouest (CEDEAO) relatif à la protection des données à caractère personnel sans toutefois pouvoir en tenir compte dans son analyse, n'ayant été en mesure de se procurer copie de sa publication au Journal officiel du Burkina Faso.

La loi définit dans son article 3 le « traitement de données à caractère personnel », soit *« toute opération ou ensemble d'opérations effectuées à l'aide de procédés automatisés ou non par une personne physique ou morale, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction »*. Cette définition correspond à celle donnée par l'article 2.b de la Convention 108.

F. Responsable du traitement/maître du fichier (article 2.d de la Convention)

La loi définit dans son article 4 alinéa 1 le « responsable du traitement », comme étant : *« la personne physique ou morale, publique ou privée, qui a le pouvoir de décider de la création des données à caractère personnel »*. Il serait opportun d'élargir cette définition afin de ne pas limiter la qualification du responsable du traitement au seul critère de « création » du traitement et reprendre les autres éléments de l'article 2.d de la Convention 108 qui fait référence à celui ou celle compétent « pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées ».

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

L'article 1 de la loi protège les personnes en matière de traitement de données « *quels qu'en soient les responsables* » (à savoir que le responsable du traitement relève du secteur public ou privé). Par ailleurs l'article 4.1 fait référence aux responsables du traitement relevant du secteur public ou privé. Enfin, l'article 18 traite spécifiquement des traitements dans le secteur public. Ce champ d'application correspond à celui énoncé à l'article 3 de la Convention 108 mais mériterait d'être clarifié de façon expresse.

L'article 8 prévoit par ailleurs que la loi s'applique *« aux traitements automatisés, ou non automatisés, de données à caractère personnel contenues ou appelées à figurer dans les fichiers dont le responsable est établi sur le territoire du Burkina Faso ou, sans y être établi, recourt à des moyens de traitement situés sur le territoire du Burkina Faso, à l'exclusion des données qui ne sont utilisées qu'à des fins de transit »*.

De plus, les dispositions des articles 12, 13, 15, 18, 19, 22 et 25 de la loi sur la collecte, l'enregistrement et la conservation des données à caractère personnel s'appliquent aux fichiers non automatisés ou mécanographiques autres que ceux dont l'usage relève de la stricte vie privée (article 57) ; pour ces fichiers, s'appliquent également les dispositions pénales de la loi (article 55).

Le Comité est d'avis que l'exclusion partielle prévue à l'article 10 pour les « *traitements ayant pour fin la recherche dans le domaine de la santé »* (pas d'information préalable des personnes concernées mais avis conforme de l'Autorité de contrôle) et l'exclusion complète prévue à l'article 11 de la loi pour les « *traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients »* devraient être réexaminées afin que de tels traitements bénéficient du dispositif de protection de la loi.

En outre, le Comité s'interroge sur l'articulation de l'exclusion complète du champ d'application de la loi des « *traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients »* (article 11) avec les dispositions de l'article 17 (deuxième paragraphe) sur le droit d'accès indirect des personnes concernées aux données à caractère médical, et de l'article 20 sur l'interdiction du traitement des données sensibles – dont les données de santé - sans le consentement des personnes concernées, sauf cas prévu à l'article 21 de la loi (le dernier tiret autorise les traitements mis en œuvre « *aux fins de médecine préventive, de diagnostics médicaux, d'administration de soins ou de traitements* » dès lors qu'ils sont effectués par des personnes soumises au secret médical).

15. Qualité des données (article 5 de la Convention)

Les articles 5, 12 et 14 contiennent les principes fondamentaux de la protection des données. « *Tout traitement des données à caractère personnel doit avoir reçu le consentement de la ou des personnes concernées, sauf dérogation prévue par la loi* » (article 5) dont celles prévues à l'article 21. Il convient de noter que la loi ne qualifie par les critères du consentement. Le responsable du traitement des données à caractère personnel doit traiter les données de manière loyale, licite et non frauduleuse (article 12). Le traitement des données doit s'effectuer à des fins « *déterminées, explicites et légitimes ; les données doivent*

être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées puis traitées ; elles doivent être conservées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées ou traitées ; au-delà, elles ne peuvent être conservées sous une forme nominative qu'en vue de leur traitement à des fins historiques, statistiques ou de recherche » (article 14). Les dispositions des articles 5, 12 et 14 sont conformes à celles de l'article 5 de la Convention 108.

L'opportunité de faire référence au fait que la personne concernée soit identifiable plutôt que de faire référence à la forme « nominative » de conservation des données pourrait être soulevée.

Enfin, le principe d'exactitude des données devrait être expressément mentionné (l'article 17.3 prévoit le droit pour la personne concernée de demander la correction ou la rectification de ses données mais la loi ne pose pas le principe de base de l'exactitude des données).

16. Catégories particulières de données (article 6 de la Convention)

La loi énonce dans son article 20 les « données sensibles », à savoir : les *« données à caractère personnel qui sont relatives à la santé [...] ou qui font apparaître les origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale ou les mœurs »*. Les données relatives aux infractions sont expressément mentionnées dans l'article 22. A l'exception de l'absence de référence explicite aux données relatives à la vie sexuelle, les catégories particulières de données prévues par la loi sont conformes à l'article 6 de la Convention 108.

L'article 20 de la loi contient le principe fondamental de l'interdiction du traitement des « données sensibles », sauf dérogation légale et mise en place de garanties appropriées. Ainsi, le traitement des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peut être effectué que par les juridictions et autorités publiques dans le cadre de leurs attributions légales, par les personnes morales gérant un service public après avis conforme de l'Autorité de contrôle, par les auxiliaires de justice pour les stricts besoins de l'exercice de leurs missions (article 22). La particularité du traitement des données à caractère personnel dans le domaine de la santé est prévue aux articles 10, 11, 17 alinéas 2 et 3, 21 sixième tiret, 23 (qui spécifie que la divulgation ou l'exploitation commerciale des données de santé à caractère personnel est interdite) et 56 de la loi. En ses dispositions pertinentes, la loi est conforme à l'article 6 de la Convention 108.

17. Sécurité des données (article 7 de la Convention)

Selon l'article 15 de la loi, « *le responsable du traitement doit mettre en œuvre toutes mesures techniques ou d'organisation appropriées afin de préserver la sécurité des données, notamment protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé* ». Cette disposition est conforme à l'article 7 alinéa 1 de la Convention 108.

18. Garanties complémentaires pour la personne concernée (article 8.a à 8.d de la Convention)

« *Le responsable du traitement de données à caractère personnel a l'obligation d'informer la personne concernée de la finalité du traitement, des destinataires des données, du caractère obligatoire ou facultatif des réponses aux questions posées ainsi que des conséquences éventuelles d'un défaut de réponse* » (article 13 al.1). Par ailleurs, le Comité salue le droit prévu à l'article 6 pour toute personne « *[…] de connaître et de contester les informations et les raisonnements utilisés dans les traitements, automatisés ou non, dont les résultats lui sont opposés* ». Les dispositions de la loi sont conformes à l'article 8.a de la Convention 108.

Les personnes concernées ont le droit de connaître les données conservées qui les concernent, et cela, sans délai ou frais excessifs (article 17.1). S'agissant des données médicales, l'article 17.2 qui prévoit l'exercice systématique du droit d'accès de façon indirecte par l'intermédiaire d'un médecin pourrait être tempéré afin de limiter cet accès indirect à certaines situations seulement.

Le droit de rectification est visé par l'article 17.3, « *s'il s'avère que des données sont incomplètes ou inexactes, les personnes concernées peuvent en demander la correction ou la rectification* ». L'article 16

paragraphe 2 mentionne le droit d'opposition (*« les personnes concernées ont le droit de s'opposer, pour des raisons légitimes, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement »*). Les dispositions de la loi sont conformes aux articles 8.b à 8.d de la Convention 108.

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

La loi prévoit des dérogations et restrictions limitées. Une limitation des droits de la personne concernée est prévue à l'article 17.4 en ce qui concerne « *les traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique* », avec exercice indirect de ces droits par l'intermédiaire de l'Autorité de contrôle. D'autre part, la loi prévoit que certaines dispositions ne sont pas applicables aux traitements faits par la presse si elles ont pour effet de limiter l'exercice de la liberté d'expression (article 25). Les dispositions de la loi sont conformes à l'article 9 de la Convention 108.

20. Sanctions et recours (article 8.d et 10 de la Convention)

S'agissant des sanctions, la loi en prévoit plusieurs aux titres III (article 37) et IV (articles 46 à 54). Elles varient de un mois à 5 ans de prison et de 200 000 à 500 000 francs CFA.

Par ailleurs, le pouvoir de l'Autorité de contrôle d'émettre des avertissements adressés aux intéressés et de dénoncer au parquet les infractions dont elle a connaissance est prévu à l'article 37.d. Les personnes peuvent porter plainte devant l'autorité de contrôle (article 37.f) ou devant la justice. En cas d'avis défavorable de l'Autorité de contrôle sur un projet de traitement à mettre en œuvre pour le compte de l'Etat, le responsable du traitement peut selon l'article 19 saisir le Conseil d'Etat. De façon générale, toute décision de l'Autorité de contrôle peut faire l'objet d'un recours.

Ces dispositions sont conformes à l'article 10 de la Convention 108.

21. Flux transfrontières de données à caractère personnel (article 12 de la Convention et article 2 du Protocole additionnel)

L'article 24 dispose que la transmission de données à caractère personnel entre le territoire burkinabé et l'étranger faisant l'objet d'un traitement automatisé régi par l'article 19 (secteur privé) ne peut s'effectuer que dans le respect de la protection assurée par la loi, sauf circonstance exceptionnelle (notion dont il conviendrait d'obtenir la portée en se basant sur la pratique de l'Autorité de contrôle en la matière) et autorisation de la transmission par un décret pris après avis conforme de l'Autorité de contrôle. Le Comité recommande que les dispositions de l'article 24 soient revues afin de mieux encadrer les transferts de données à l'étranger.

S'agissant des flux transfrontières en matière de traitements relevant du secteur public, c'est l'article 18 qui s'applique, qui prévoit également l'avis conforme de l'Autorité de contrôle.

22. Autorité de contrôle (article 1er du Protocole additionnel)

La loi prévoit l'établissement d'une Autorité de contrôle, dénommée « Commission de l'informatique et des libertés » visée par le Titre II ainsi que par les articles 10, 17 alinéa 4, 18, 19, 22 deuxième tiret, 24 alinéa 2, 52, 56 alinéa 1 et 59 de la loi. La Commission est une autorité administrative indépendante dont la création, la composition, le statut des membres, le budget, les attributions larges (dont des pouvoirs *a priori* et le pouvoir d'investigation), la publicité de traitements mis œuvre, le rapport annuel sont précisés respectivement aux articles 26, 27, 28 à 34, 35 et 36, 37 à 43, 44, 45. La Commission est composée d'un collège de neuf membres nommés en Conseil des Ministres, après élections ou désignations par leurs pairs des différents corps ou associations auxquels ils appartiennent, pour garantir l'indépendance de l'Autorité de contrôle. Les membres ne peuvent être ni membre du gouvernement ni responsable d'entreprise. En outre, ils prêtent serment d'indépendance et d'impartialité.

Ces dispositions satisfont à l'article 1er du Protocole additionnel à la Convention 108.

Il convient par ailleurs de noter que la CIL qui a été établie en décembre 2007 peut présenter le bilan suivant (depuis 2008) :

DESIGNATION	**NOMBRE**
NOMBRE DE STRUCTURES DONT LES DOSSIERS ONT ETE TRAITES	61 STRUCTURES
DEMANDES DE CONSEILS	50 DOSSIERS
DECLARATIONS NORMALES	144 TRAITEMENTS
AUTORISATIONS DE TRANSFERT	45 TRAITEMENTS
DEMANDES D'AVIS	14 TRAITEMENTS
PLAINTES	40 PLAINTES FORMELLES TRAITEES

Remarques complémentaires

Les dispositions de la loi ne s'appliquent pas *« aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique en vue du stockage automatique intermédiaire et transitoire des données à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations »* (article 9). Le Comité souligne qu'une telle exception n'est admissible qu'à condition que les données ne soient conservées que pendant une très courte période et que les copies temporaires soient effacées une fois l'acheminement effectué.

Le Comité salue les dispositions de l'article 7, « *Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé destiné à évaluer certains aspects de sa personnalité. Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain, ne peut avoir pour seul fondement un traitement automatisé d'informations, donnant une définition du profil ou de la personnalité de l'intéressé* ».

Conclusion

Eu égard à ce qui précède, le Comité estime que la loi du Burkina Faso sur la protection des données, tout en méritant de faire l'objet des aménagements notés dans le présent avis, *satisfait de manière générale* aux règles de la Convention 108 et de son Protocole additionnel. Aussi le Comité consultatif, se basant sur l'analyse de la législation applicable en matière de protection des données, est d'avis que la demande du Burkina Faso d'être invité à adhérer à la Convention 108 et à son Protocole additionnel devrait être reçue favorablement.