
Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, Adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990

Les modalités d'application des règlements concernant les fichiers informatisés contenant des données à caractère personnel sont laissées à la libre initiative de chaque Etat sous réserve des orientations suivantes:

A. Principes concernant les garanties minimales qui devraient être prévues dans les législations nationales

1. Principe de licéité et de loyauté

Les données concernant les personnes ne devraient pas être obtenues ou traitées à l'aide de procédés illicites ou déloyaux, ni utilisées à des fins contraires aux buts et aux principes de la Charte des Nations Unies.

2. Principe d'exactitude

Les personnes responsables de l'établissement d'un fichier ou celles responsables de leur mise en oeuvre devraient être tenues de vérifier l'exactitude et la pertinence des données enregistrées et de veiller à ce qu'elles demeurent aussi complètes que possible pour éviter les erreurs par omission et qu'elles soient mises à jour, périodiquement ou lors de l'utilisation des informations contenues dans un dossier, tant qu'elles font l'objet d'un traitement.

3. Principe de finalité

La finalité en vue de laquelle est créé un fichier et son utilisation en fonction de cette finalité devraient être spécifiées, justifiées et, lors de sa mise en oeuvre, faire l'objet d'une mesure de publicité ou être portées à la connaissance de la personne concernée, afin qu'il soit ultérieurement possible de vérifier:

- a) Si toutes les données personnelles collectées et enregistrées restent pertinentes par rapport à la finalité poursuivie;
- b) Si aucune desdites données personnelles n'est utilisée ou divulguée, sauf accord de la personne concernée, à des fins incompatibles avec celles ainsi spécifiées;
- c) Si la durée de conservation des données personnelles n'excède pas celle permettant d'atteindre la finalité pour laquelle elles ont été enregistrées.

4. Principe de l'accès par les personnes concernées

Toute personne justifiant de son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs, d'obtenir les rectifications ou destructions adéquates en cas d'enregistrements illicites, injustifiés ou inexacts, et,

lorsqu'elles sont communiquées, d'en connaître les destinataires. Une voie de recours devrait être prévue, le cas échéant, auprès de l'autorité de contrôle prévue au principe 8 ci-dessous. En cas de rectification, le coût devrait être à la charge du responsable du fichier. Il est souhaitable que les dispositions de ce principe s'appliquent à toute personne, quelle que soit sa nationalité ou sa résidence.

5. Principe de non-discrimination

Sous réserve des cas de dérogations limitativement prévus sous le principe 6, les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées.

6. Faculté de dérogation

Des dérogations aux principes 1 à 4 ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées.

Les dérogations au principe 5 relatif à la prohibition de la discrimination, outre qu'elles devraient être soumises aux mêmes garanties que celles prévues pour les dérogations aux principes 1 à 4, ne pourraient être autorisées que dans les limites prévues par la Charte internationale des droits de l'homme et les autres instruments pertinents dans le domaine de la protection des droits de l'homme et de la lutte contre les discriminations.

7. Principe de sécurité

Des mesures appropriées devraient être prises pour protéger les fichiers tant contre les risques naturels, tels que la perte accidentelle ou la destruction par sinistre, que les risques humains, tels que l'accès non autorisé, l'utilisation détournée de données ou la contamination par des virus informatiques.

8. Contrôle et sanctions

Chaque législation devrait désigner l'autorité qui, en conformité avec le système juridique interne, est chargée de contrôler le respect des principes précités. Cette autorité devrait présenter des garanties d'impartialité, d'indépendance à l'égard des personnes ou organismes responsables des traitements et de leur mise en oeuvre, et de compétence technique. En cas de violation des dispositions de la loi interne mettant en oeuvre les principes précités, des sanctions pénales ou autres devraient être prévues ainsi que des recours individuels appropriés.

9. Flux transfrontières de données

Lorsque la législation de deux ou plusieurs pays, concernés par un flux transfrontières de données, présente des garanties comparables au regard de la protection de la vie privée, les informations doivent pouvoir circuler aussi librement qu'à l'intérieur de chacun des territoires concernés. En l'absence de garanties comparables, des limitations à cette circulation ne peuvent être imposées indûment et seulement dans la stricte mesure où la protection de la vie privée l'exige.

10. Champ d'application

Les présents principes devraient s'appliquer en premier lieu à tous les fichiers informatisés publics et privés et, par voie d'extension facultative et sous réserve des adaptations adéquates, aux fichiers traités manuellement. Des dispositions particulières également facultatives pourraient être prises pour étendre tout ou partie desdits principes aux fichiers de personnes morales, notamment lorsqu'ils contiennent pour partie des informations concernant des personnes physiques.

B. Application des principes directeurs aux fichiers contenant des données à caractère personnel, détenus par les organisations internationales gouvernementales

Les présents principes directeurs devraient être applicables aux fichiers contenant des données à caractère personnel détenus par les organisations internationales gouvernementales sous réserve des adaptations nécessaires pour tenir compte des différences qui peuvent exister entre les fichiers à finalités internes tels que ceux qui concernent la gestion du personnel et les fichiers à finalités externes concernant les tiers en relation avec l'organisation.

Chaque organisation devrait désigner l'autorité statutairement compétente pour contrôler la bonne application des présents principes directeurs.

Clause humanitaire: une dérogation à ces principes devrait être spécifiquement prévue lorsque le fichier a pour finalité la protection des droits de l'homme et des libertés fondamentales de la personne concernée ou l'assistance humanitaire.

Une dérogation de même portée devrait être prévue dans la loi nationale en faveur des organisations internationales gouvernementales dont l'accord de siège n'aurait pas écarté l'application de ladite législation nationale, ainsi qu'en faveur des organisations internationales non gouvernementales auxquelles ladite loi serait applicable.