COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 16 mars 2016 T-PD-BUR(2015)12Rev2

BUREAU DU COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

(T-PD-BUR)

Projet de lignes directrices sur la protection des individus à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées

Direction générale Droits de l'homme et État de droit

I. Introduction

Les présentes lignes directrices tiennent compte des différences entre les Parties concernant le cadre législatif de la protection des données et ont été rédigées sur la base de la Convention 108, dans le cadre du processus continu de modernisation de cet instrument. Elles s'adressent principalement aux autorités de réglementation, aux responsables du traitement des données et aux sous-traitants, tels que définis à la section III.

Le préambule du projet de Convention modernisée s'attache à la protection de « l'autonomie personnelle, fondée sur le droit de toute personne de contrôler ses propres données à caractère personnel et du traitement qui en est fait ». La nature de ce droit de contrôle devrait faire l'objet d'une attention particulière sous l'angle de l'utilisation des mégadonnées (*Big Data*).

Le contrôle suppose que la personne concernée soit informée de l'utilisation des données et qu'elle ait une réelle liberté de choix. Ces conditions, essentielles à la protection des droits fondamentaux, peuvent être satisfaites en recourant à diverses solutions juridiques qui devraient être adaptées au contexte social et technologique en tenant compte du déficit de connaissance des individus.

La complexité et l'opacité des applications utilisant des mégadonnées devraient donc inciter les autorités de réglementation à considérer que la notion de contrôle ne se limite pas à un simple contrôle individuel (par exemple par le biais du dispositif de notification et consentement). Lesdites autorités devraient adopter une conception plus large du contrôle de l'utilisation des données, en vertu de laquelle le contrôle individuel évolue en un processus plus complexe d'évaluation – sous plusieurs aspects – des risques liés à l'utilisation des données.

II. Champ d'application

Les présentes lignes directrices recommandent des mesures que les Parties, les responsables du traitement des données et les sous-traitants devraient prendre pour prévenir l'impact potentiel négatif de l'utilisation des mégadonnées sur la dignité humaine, les droits de l'homme et les libertés fondamentales individuelles et collectives, principalement en ce qui concerne la protection des données.

Compte tenu de la nature des mégadonnées, l'application de certains principes traditionnels du traitement de données (principe de minimisation, finalités déterminées, consentement valable, etc.) pourrait poser des difficultés dans ce scénario technologique. Les présentes lignes directrices suggèrent par conséquent une application adaptée des principes de la Convention 108, afin de renforcer leur efficacité en pratique dans le contexte des mégadonnées.

L'objet des présentes lignes directrices est de définir des principes et des pratiques de nature à limiter les risques liés à l'utilisation de mégadonnées. Ces risques sont principalement liés au caractère potentiellement biaisé de l'analyse des données, à la

sous-estimation des implications sociales et éthiques du recours aux mégadonnées pour prendre des décisions et à la marginalisation d'une participation réelle et consciente des individus à ces processus.

Les présentes lignes directrices concernant les mégadonnées en général et non des applications propres à un secteur, elles énoncent des orientations générales et de haut niveau qui pourraient être complétées par d'autres lignes directrices relatives à la protection des individus dans des domaines d'application spécifiques des mégadonnées (comme la santé ou la finance).

Rien dans les présentes lignes directrices ne saurait être interprété comme excluant ou limitant les dispositions de la Convention 108 et les garanties mises en place dans cet instrument en faveur de la personne concernée.

III. Terminologie utilisée dans les présentes lignes directrices :

a) **Mégadonnées** : les définitions de ce terme sont nombreuses et diffèrent selon la discipline spécifique considérée. La plupart d'entre elles se concentrent sur la capacité technologique croissante de collecter, traiter et extraire très rapidement des connaissances prédictives à partir d'un gros volume et d'une grande variété de données. Néanmoins, sous l'angle de la protection des données, les principaux problèmes ne viennent pas uniquement du volume et de la variété des données traitées et de la vitesse du processus, mais également de l'analyse de ces données au moyen d'un logiciel dans le but d'extraire des connaissances prédictives de nature à orienter un processus décisionnel. Aux fins des présentes lignes directrices, la définition des mégadonnées englobe donc à la fois les données elles-mêmes et leur analytique.

b) **Projet de convention modernisée** : le projet de version modernisée de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (texte consolidé, tel qu'il a été révisé en janvier 2016).

c) **Parties** : les parties ayant ratifié, accepté ou approuvé la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Strasbourg, 28 janvier 1981).

d) **Données à caractère personnel** : toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel englobent également toute information utilisée pour prendre des décisions touchant un individu appartenant à un groupe sur la base d'un profilage de ce groupe.

e) **Processus d'évaluation des risques** : le processus décrit plus bas à la section IV.2.

f) **Données sensibles** : données appartenant aux catégories énumérées à l'article 6 de la Convention 108. Les données ne révélant pas directement d'informations sensibles, mais susceptibles de le faire en cas de traitement supplémentaire ou en

combinaison avec d'autres données, sont considérées comme sensibles.

g) **Autorité de surveillance** : autorité indépendante établie par une Partie en vertu de l'article 13.2 de la Convention 108.

IV. Principes et lignes directrices

1. Utilisation des données soucieuse des incidences éthiques et sociales

1.1 En vertu du principe de juste équilibre entre tous les intérêts concernés dans le cadre du traitement de données à caractère personnel, dès lors que l'information sert à faire des prévisions pour orienter des processus de décision, les responsables du traitement des données et les sous-traitants devraient tenir dûment compte des implications éthiques et sociales plus larges des mégadonnées, en vue de garantir le respect intégral des obligations en matière de protection des données énoncées par la Convention 108 et de garantir l'exercice des droits fondamentaux.

1.2 L'utilisation des données ne saurait aller à l'encontre des valeurs éthiques communément acceptées dans le milieu ou les milieux compétents ou porter atteinte à des intérêts sociétaux, y compris la protection des droits de l'homme. Même si la définition de règles éthiques prescriptives risque de s'avérer problématique, en raison de l'influence de facteurs contextuels, les valeurs éthiques communément reconnues figurent dans les instruments internationaux de protection des droits de l'homme et des libertés fondamentales comme la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

1.3 Si le processus d'évaluation des risques révèle un fort impact de l'utilisation des mégadonnées sur les valeurs éthiques, les responsables du traitement des données peuvent établir un comité ad hoc chargé d'identifier les valeurs éthiques spécifiques qu'il convient de protéger dans le cadre de l'utilisation de ces données.

2. Politiques préventives et évaluation des risques

2.1 Compte tenu de la complexité croissante du traitement des données et de l'utilisation transformative des mégadonnées, les Parties devraient adopter une approche de précaution en matière de réglementation de la protection des données dans ce domaine.

2.2 Les responsables du traitement des données devraient adopter des politiques préventives concernant les risques liés à l'utilisation des données et à l'impact de cette utilisation sur les individus et la société.

2.3 En vertu de l'article 5.1 et de l'article 8*bis*.2 du projet de Convention modernisée, une évaluation des risques de l'impact potentiel du traitement des données sur les droits et libertés fondamentaux s'impose, de manière à mettre en balance les différents intérêts concernés par l'utilisation des mégadonnées.

2.4 L'utilisation des mégadonnées pouvant porter atteinte non seulement à la vie privée et à la protection des données des individus, mais également la dimension collective de ces droits, les politiques préventives et l'évaluation des risques devraient tenir compte de

l'impact social et éthique de cette utilisation, y compris sous l'angle du droit d'être traité sur un pied d'égalité, sans discrimination aucune.

2.5 Les responsables du traitement des données devraient mener un processus d'évaluation des risques afin :

1) d'identifier les risques ;
2) d'évaluer les risques de chaque application spécifique utilisant des mégadonnées et de ses incidences potentiellement négatives sur les droits et libertés des individus, en particulier le droit à la protection des données à caractère personnel et le droit à la non-discrimination, en tenant compte des impacts sociaux et éthiques ;
3) de prévoir des remèdes adéquats en intégrant dans les applications des solutions technologiques conçues pour atténuer ces risques ;
4) de surveiller l'adoption et l'efficacité des solutions proposées.

2.6 Le processus d'évaluation des risques devrait être mené par des personnes dotées des qualifications professionnelles et des connaissances adéquates pour apprécier les différents impacts, y compris dans leurs dimensions sociale et éthique.

2.7 En ce qui concerne l'utilisation de mégadonnées susceptible de porter atteinte aux droits fondamentaux, les Parties devraient encourager la participation des différents acteurs au processus d'évaluation des risques et à la conception du traitement des données.

2.8 Les responsables du traitement des données devraient examiner, à intervalles réguliers, les résultats du processus d'évaluation des risques.

2.9 Les responsables du traitement des données devraient documenter l'évaluation et les solutions mentionnées au paragraphe 2.5.

2.10 Les autorités de surveillance devraient formuler des recommandations à l'intention des responsables du traitement des données sur les méthodes de pointe en matière de sécurité du traitement des données, ainsi que des lignes directrices sur le processus d'évaluation des risques.

2.11 Les Parties peuvent introduire certaines limites à la responsabilité des responsables du traitement des données en matière d'indemnisation des dommages résultant des risques mentionnés au paragraphe 2.5, dès lors que les responsables ont traité les données à caractère personnel conformément aux dispositions de cet article.

3. Détermination des finalités et transparence

3.1 Compte tenu de la nature transformative de l'utilisation des mégadonnées, le traitement devrait avoir des finalités explicites et déterminées, conformément à l'article 5.b de la Convention 108 et à l'article 5.4.b du projet de version modernisée du même instrument, et identifier également l'impact potentiel des différentes utilisations des données sur les individus.

3.2 En vertu de l'article 7*bis*.1 du projet de convention modernisée, les résultats du

processus d'évaluation des risques devraient être rendus publics, sans préjudice du secret protégé par la loi. En présence d'un tel secret, les responsables du traitement des données devraient communiquer toute information sensible éventuelle dans une annexe séparée du rapport d'évaluation, laquelle ne serait pas rendue publique, mais pourrait être consultée par les autorités de surveillance.

3.3 Lorsque les données réunies font l'objet d'un traitement supplémentaire à des fins historiques, statistiques ou scientifiques, elles ne devraient être stockées sous une forme permettant l'identification des personnes concernées au-delà de la période considérée comme nécessaire. Dans certains de ces cas de figure, les garanties appropriées peuvent inclure la restriction de l'accès et/ou de la disponibilité publique des données dès lors que, en vertu de la loi, l'accès à cette information ne répond à aucun intérêt public ou individuel légitime.

4. Solutions dès la conception

4.1 Sur la base du processus d'évaluation des risques, les responsables du traitement des données et les sous-traitants devraient adopter des solutions adéquates dès la conception, aux différents stades du traitement des mégadonnées.

4.2 Les responsables du traitement des données et les sous-traitants devraient soigneusement examiner la conception de leur analyse de données, de manière à éviter tout biais caché potentiel susceptible d'affecter aussi bien la collecte que l'analyse et d'éliminer un maximum de données redondantes ou marginales.

4.3 Lorsque cela est techniquement faisable, les responsables du traitement des données et les sous-traitants devraient tester l'adéquation de leurs solutions adoptées dès la conception sur un volume limité de données au moyen de simulations, avant leur utilisation à une plus grande échelle. Une telle approche permettrait d'évaluer tout biais potentiel dans l'utilisation des différents paramètres d'analyse des données et d'apporter des éléments en vue de minimiser l'utilisation des informations et de réduire les incidences négatives potentielles identifiées dans le cadre du processus d'évaluation des risques.

4.4 En ce qui concerne l'utilisation des données sensibles, des solutions dès la conception devraient être adoptées de manière à éviter que des données non sensibles servent à déduire des informations sensibles, et, le cas échéant, à étendre à ces données les mêmes garanties que celles applicables aux données sensibles.

5. Consentement

5.1 Compte tenu de la complexité de l'utilisation des mégadonnées, le consentement, pour être valable, devrait se fonder sur les informations communiquées à la personne concernée en vertu de l'article 7*bis* du projet de convention modernisée. Cette information devrait comprendre les résultats du processus d'évaluation des risques et pourrait également être communiquée au moyen d'une interface simulant les effets de l'utilisation des données et son impact potentiel sur la personne concernée, dans le cadre d'une

approche d'apprentissage par l'expérience.

5.2 Une fois les données collectées sur la base du consentement de la personne concernée, elles ne peuvent plus être traitées d'une manière incompatible avec les finalités initiales. Les responsables du traitement des données et les sous-traitants devraient fournir aux personnes concernées un moyen technique accessible et d'utilisation facile pour retirer leur consentement et s'opposer à tout traitement des données incompatible avec les finalités initiales.

5.3 En vertu de l'article 5.b de la Convention 108, le traitement des données est considéré comme incompatible dès lors que l'utilisation desdites données expose les personnes concernées à des risques supérieurs ou différents par rapport à ceux prévus dans les finalités initiales.

5.4 Le consentement n'est pas donné librement en cas de déséquilibre entre les pouvoirs conférés aux responsables du traitement des données ou aux sous-traitants et ceux de la personne concernée. Le responsable des données devrait démontrer qu'il n'existe pas de déséquilibre dans ce domaine ou que le déséquilibre existant n'a pas d'incidence sur le consentement donné par la personne concernée.

6. Anonymisation

6.1 Dans le contexte des mégadonnées, le caractère anonyme des données traitées n'exclut pas, en règle générale, l'application des principes relatifs à la protection des données, dans la mesure où il existe un risque de ré-identification.

6.2 L'anonymisation peut combiner des mesures techniques avec des obligations juridiques ou contractuelles interdisant toute tentative de ré-identification des données.

6.3 Compte tenu du risque de ré-identification, le responsable du traitement des données devra démontrer, preuves à l'appui, l'adéquation des mesures d'anonymisation. Cette évaluation du risque de ré-identification devra tenir compte à la fois de la nature des données et du coût de la mise en œuvre des techniques d'anonymisation disponibles.

7. Rôle du facteur humain dans les prises de décision reposant sur les mégadonnées

7.1 L'utilisation de mégadonnées devrait préserver l'autonomie du facteur humain dans le processus décisionnel.

7.2 Les décisions fondées sur les résultats fournis par l'analyse des mégadonnées devraient tenir compte de toutes les particularités des données et ne pas se fonder simplement sur des informations ou des résultats de traitements décontextualisés.

7.3 Lorsque des décisions fondées sur des mégadonnées risquent de porter atteinte aux droits individuels, un décideur en chair et en os doit expliquer les raisons de ces décisions à la personne concernée de manière détaillée.

7.4 Sur la base d'arguments raisonnables, le décideur en chair et en os devrait se voir

conférer la liberté de ne pas suivre les recommandations découlant de l'utilisation des mégadonnées.

7.5 En présence d'un soupçon de discrimination directe ou indirecte fondée sur les recommandations issues des mégadonnées, les responsables du traitement des données et les sous-traitants devraient apporter la preuve de l'absence de discrimination.

7.6 Les personnes affectées par une décision fondée sur des mégadonnées ont le droit de contester celle-ci devant une autorité compétente.

8. Données ouvertes

8.1 Compte tenu de la disponibilité des outils d'analyse de mégadonnées, les personnes physiques et morales devraient examiner minutieusement leurs politiques de données ouvertes en ce qui concerne les données à caractère personnel. Lorsque des responsables du traitement des données adoptent une politique ouverte, le processus d'évaluation des risques devrait prendre en considération les effets de la fusion et de l'exploration de données relevant de différents ensembles de données ouvertes.

9. Dérogations à des fins historiques, statistiques et scientifiques

9.1 Lorsque les Parties accordent des dérogations spécifiques aux dispositions des articles 7*bis* et 8 du projet de convention modernisée en matière de traitement des données à des fins historiques, statistiques et scientifiques, elles devraient exclure tout risque de violation des droits et des libertés fondamentales des personnes concernées.

9.2 Les dérogations devraient être limitées au strict nécessaire et n'être appliquées que si elles sont strictement prévues par la loi.

9.3 Les dérogations ne sauraient porter atteinte aux droits fondamentaux, au principe de non-discrimination et au droit des personnes concernées de contester devant une autorité compétente toute décision prise sur la base d'un traitement automatisé des données.

10. Éducation

10.1 Pour aider les citoyens à comprendre les implications de l'utilisation d'informations et de données à caractère personnel dans le contexte des mégadonnées, les Parties devraient considérer la maîtrise du numérique comme un élément essentiel de l'éducation et l'inclure dans les programmes standard.