Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées

www.coe.int/data-protection

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 23 janvier 2017 T-PD(2017)01

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

(T-PD)

Lignes directrices[1] sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées[2]

Direction générale droits de l'Homme et État de droit

[1] Sur les 50 membres votant, abstention du Danemark, Liechtenstein et du Luxembourg, et objection de l'Allemagne et de l'Irlande.

[2] Le projet initial et les versions révisées des lignes directrices ont été préparés par Alessandro Mantelero, professeur agrégé titulaire à l'École polytechnique de Turin (Italie).

I. Introduction

Les mégadonnées (*Big Data*) constituent un nouveau paradigme de la manière dont les informations sont collectées, combinées et analysées. Les mégadonnées, qui tirent profit d'interactions avec d'autres environnements technologiques tels que l'internet des objets et le *cloud*, peuvent être source de grande valeur et d'innovation pour la société en permettant d'accroître la productivité, les performances du secteur public et la participation sociale.

Les éclairages précieux fournis par les mégadonnées changent notre façon de comprendre et d'organiser la société. Toutes les données traitées dans le cadre de traitements de mégadonnées ne sont pas nécessairement des données à caractère personnel ou relatives aux interactions sociales mais un large spectre de données en relève, ayant un effet direct sur les personnes et leurs droits à l'égard du traitement des données à caractère personnel.

Par ailleurs, en raison des possibilités offertes par les mégadonnées de collecter et d'analyser de vastes quantités de données afin d'identifier des tendances et de prédire des comportements de groupes et de communautés, la dimension collective des risques liés à l'utilisation des données est également à considérer.

C'est pourquoi le Comité de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108, ci-après la « Convention 108 ») a été amené à rédiger les présentes lignes directrices, qui définissent un cadre général permettant aux Parties de concevoir des politiques et des mesures de nature à rendre effectifs les principes et les dispositions de la Convention 108 dans le contexte des mégadonnées.

Les présentes lignes directrices ont été rédigées sur la base des principes de la Convention 108, au vu du processus de modernisation de cet instrument, et s'adressent principalement aux autorités de réglementation, aux responsables du traitement et aux sous-traitants, tels que définis à la section III.

Etant donnée la nécessité d'assurer la protection de l'autonomie personnelle, fondée sur le droit de toute personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait, la nature de ce droit de contrôle devrait faire l'objet d'une attention particulière lorsque les données à caractère personnel sont traitées dans un contexte de mégadonnées.

Le contrôle suppose que la personne concernée soit informée de l'utilisation des données à caractère personnel et qu'elle ait une réelle liberté de choix. Ces conditions, essentielles à la protection des droits fondamentaux, en particulier du droit fondamental à la protection des données à caractère personnel, 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 personnes.

La complexité et l'opacité des applications utilisant des mégadonnées devraient donc inciter ceux chargés d'édicter les règles à considérer que la notion de contrôle ne se limite pas à un simple contrôle individuel. Ils 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 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, notamment en ce qui concerne la protection des données à caractère personnel.

Compte tenu de la nature des mégadonnées et de leur utilisation, l'application de certains principes traditionnels du traitement de données (principe de minimisation des données ; de finalité ; de loyauté et de transparence ; consentement libre, spécifique et éclairé) pourrait poser des difficultés dans ce scénario technologique. Les présentes lignes directrices suggèrent par conséquent une application spécifique 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 contribuer à la protection des personnes concernées à l'égard du traitement des données à caractère personnel dans le contexte des mégadonnées en précisant les principes applicables en matière de protection des données et les pratiques correspondantes, en vue de limiter les risques que l'utilisation de mégadonnées comporte pour les droits des personnes concernées. Ces risques sont principalement liés au caractère potentiellement biaisé de l'analyse des données, à la sous-estimation des implications juridiques, sociales et éthiques du recours aux mégadonnées pour prendre des décisions et à la marginalisation d'une participation effective et éclairée des personnes à ces processus.

Compte tenu de l'ampleur expansive des mégadonnées, aux applications propres à divers secteurs, les présentes lignes directrices énoncent des orientations générales qui pourraient être complétées par d'autres orientations et des bonnes pratiques adaptées relatives à la protection des personnes dans des domaines d'application spécifiques des mégadonnées (comme dans le secteur de la santé, de la finance ou le secteur public, notamment pour les autorités chargées de l'application de la loi).

Par ailleurs, le texte actuel des lignes directrices pourra à l'avenir être révisé si cela est jugé nécessaire par le Comité de la Convention 108 à la lumière des évolutions en matière technologique et des utilisations faites de ces technologies.

Rien dans les présentes lignes directrices ne saurait être interprété comme excluant ou limitant les dispositions de la Convention 108 et de la Convention européenne des droits de l'homme.

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 nouvelles et prédictives à partir d'un gros volume, d'une grande variété de données et à une vélocité considérable[3]. Sous l'angle de la protection des données, les principaux problèmes ne viennent pas uniquement du volume, 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 à l'égard de personnes ou de groupes. Aux fins des présentes lignes directrices, la définition des mégadonnées englobe donc à la fois les données elles-mêmes et le procédé analytique[4].

b) **Responsable du traitement** : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ;

c) **Sous-traitant** : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

d) **Traitement de données** : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données.

[3] Le terme « mégadonnées » désigne ordinairement des ensembles de données extrêmement volumineux qui peuvent être analysés par ordinateur en vue d'en extraire des inférences statistiques sur les schémas, les tendances et les corrélations de données. Selon l'Union internationale des télécommunications, les mégadonnées sont « un paradigme permettant la collecte, le stockage, la gestion, l'analyse et la visualisation, potentiellement sans délai, de vastes ensembles de données aux caractéristiques hétérogènes. » (UIT, Recommandation Y.3600, « Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage », 2015.)

[4] Cette expression sert à désigner des technologies informatiques qui analysent de grandes quantités de données en vue d'y découvrir des schémas, des tendances et des corrélations dissimulés. D'après l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'analytique des mégadonnées « renvoie à l'ensemble du cycle de gestion des données, qui comprend la collecte, l'organisation et l'analyse des données, et vise à découvrir des schémas, à inférer des situations ou des états, à prévoir et comprendre des comportements. » (ENISA, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015.)

e) **Pseudonymisation** : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

f) ***Open data*** : toute information disponible publiquement qui peut être librement utilisée, modifiée, partagée et réutilisée par quiconque et à toute fin dans le respect des conditions des licences ouvertes.

g) **Parties** : les parties tenues juridiquement par la Convention 108.

h) **Données à caractère personnel** : toute information concernant une personne physique identifiée ou identifiable (la personne concernée)[5].

i) **Données sensibles** : catégories particulières des données énumérées à l'article 6 de la Convention 108[6] requérant des garanties complémentaires appropriées lorsqu'elles sont traitées.

j) **Autorité de contrôle** : l'autorité établie par une Partie et chargée de veiller au respect des dispositions de la Convention 108.

IV. Principes et lignes directrices

1. Utilisation des données soucieuse des incidences éthiques et sociales

1.1 Dans le respect d'un juste équilibre entre tous les intérêts concernés dans le cadre du traitement de données à caractère personnel, et en particulier dès lors que l'information sert des finalités prédictives dans le cadre d'un processus de prise de décision, les responsables du traitement et les sous-traitants devraient tenir dûment compte de l'impact potentiel du traitement des mégadonnées envisagé et de ses implications éthiques et sociales plus larges, en vue de garantir les droits de l'Homme et les libertés fondamentales et d'assurer le respect des obligations en matière de protection des données, telles qu'énoncées par la Convention 108.

1.2 Le traitement des données à caractère personnel ne devrait pas aller à l'encontre des valeurs éthiques communément acceptées dans la communauté ou les communautés pertinentes, et ne devrait pas porter atteinte à des intérêts, des valeurs et des normes 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 telle que la Convention européenne des Droits de l'Homme.

1.3 Si l'évaluation de l'impact potentiel d'un traitement de données envisagé, telle que décrite à la section IV.2, révèle un fort impact de l'utilisation des mégadonnées sur les valeurs éthiques, les responsables du traitement des données peuvent établir un comité d'éthique ad hoc, ou s'appuyer sur les existants, afin d'identifier les valeurs éthiques spécifiques qu'il convient de protéger dans le cadre de l'utilisation de ces données. Le comité d'éthique devrait être un organe indépendant composé de membres choisis pour leurs compétences, leur expérience et leurs qualités professionnelles et accomplissant leur mission de façon impartiale et objective.

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

[5] Selon cette définition, les données à caractère personnel englobent également toute information utilisée pour individualiser ou singulariser des personnes identifiées sur la base d'informations relatives au profilage d'un groupe.

[6] En matière de mégadonnées, ceci est particulièrement pertinent s'agissant des informations sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle qui sont révélées dans le cadre d'un traitement ultérieur ou de combinaison avec d'autres données.

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 devraient adopter des politiques préventives concernant les risques liés à l'utilisation des mégadonnées et à l'impact de cette utilisation sur les personnes et la société, afin de garantir la protection des personnes à l'égard du traitement de données à caractère personnel.

2.3 L'utilisation des mégadonnées pouvant porter atteinte non seulement à la vie privée et à la protection des données de façon individuelle, mais également à la dimension collective de ces droits, les politiques préventives et l'évaluation des risques doivent tenir compte de l'impact juridique, social et éthique de cette utilisation, y compris au regard du droit à l'égalité de traitement et à la non-discrimination.

2.4 En vertu des principes de légitimité du traitement des données et de qualité des données, énoncés dans la Convention 108, et conformément à l'obligation de prévenir ou minimiser l'impact du traitement des données sur les droits et les libertés fondamentales des personnes concernées, une évaluation des risques de l'impact potentiel du traitement des données sur les droits et libertés fondamentales s'impose, de manière à parvenir à un juste équilibre entre la protection de ces droits et libertés et les différents intérêts concernés par l'utilisation des mégadonnées.

2.5 Les responsables du traitement devraient procéder à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées afin :

1) d'identifier et d'évaluer les risques de chaque activité de traitement de mégadonnées et de ses incidences potentiellement négatives sur les droits et libertés fondamentales des personnes, 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 ;

2) de mettre au point et de prévoir des mesures appropriées, notamment dès la conception (*by-design*) et par défaut (*by default*)[7], pour atténuer les risques qui seront identifiés ;

3) de suivre de près l'adoption et l'efficacité des solutions proposées.

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

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 (par exemple, des personnes ou groupes qui pourraient être concernés par l'utilisation des mégadonnées) au processus d'évaluation des risques et à la conception du traitement des données.

2.8 Lorsque l'utilisation des mégadonnées est susceptible d'avoir un impact important sur les droits et libertés fondamentales des personnes concernées, les responsables du traitement devraient consulter les autorités de contrôle afin de chercher à obtenir des conseils visant à réduire les risques visés au paragraphe 2.5 et tirer profit des orientations fournies par ces autorités.

2.9 Les responsables du traitement doivent examiner, à intervalles réguliers, les résultats du processus d'évaluation des risques.

2.10 Les responsables du traitement doivent documenter l'évaluation et les solutions mentionnées au paragraphe 2.5.

2.11 Les mesures adoptées par les responsables du traitement pour réduire les risques visés au paragraphe 2.5 devraient être prises en compte lors de l'évaluation d'éventuelles sanctions administratives.

[7] Dans le contexte de la protection des données, les expressions « dès la conception » (*privacy by design*) et « par défaut » (p*rivacy by default*) renvoient à des mesures technologiques et organisationnelles adéquates prises en compte dans tout le processus de gestion des données, dès les premières étapes de la conception, aux fins de la mise en œuvre effective des principes juridiques et du renforcement des garanties de protection des données dans les produits et services. Dans le cadre de l'approche « par défaut », les mesures visant à garantir les droits des personnes concernées sont la configuration de base, par défaut et permettent notamment que seules les informations à caractère personnel nécessaires à un traitement de données spécifique sont traitées.

3. Principe de finalité et transparence

3.1 Les données à caractère personnel doivent être traitées pour des finalités déterminées et légitimes, et ne doivent pas être utilisées de manière incompatible avec ces finalités. Les données à caractère personnel ne devraient pas faire l'objet d'un traitement ultérieur que la personne concernée puisse considérer comme étant inattendu, inapproprié ou contestable. Exposer la personne concernée à des risques différents ou supérieurs à ceux envisagés pour les finalités initiales pourrait être considéré comme un traitement ultérieur inattendu.

3.2 Compte tenu de la nature transformative de l'utilisation des mégadonnées, et pour satisfaire à l'exigence relative au consentement libre, spécifique, éclairé et non-équivoque, ainsi qu'aux principes de restriction, de loyauté et de transparence, les responsables du traitement devraient également identifier l'impact potentiel des différentes utilisations des données sur les personnes, et en informer les personnes concernées.

3.3 Conformément au principe de transparence du traitement, les résultats du processus d'évaluation des risques décrit à la section IV.2 devraient être rendus publics, sans préjudice d'une confidentialité protégée par la loi. En présence d'une telle confidentialité, les responsables du traitement communiquent toute information confidentielle éventuelle dans une annexe séparée du rapport d'évaluation, laquelle ne doit pas être rendue publique, mais pourrait être consultée par les autorités de contrôle.

4. Solutions dès la conception (*by-design*)

4.1 Sur la base du processus d'évaluation décrit à la section IV.2, les responsables du traitement et, le cas échéant, les sous-traitants doivent adopter des solutions adéquates dès la conception, aux différents stades du traitement des mégadonnées.

4.2 Les responsables du traitement et, le cas échéant, les sous-traitants devraient soigneusement examiner la conception du traitement de données afin de minimiser la présence de données redondantes ou marginales et d'éviter ainsi tout biais caché potentiel et tout risque de discrimination ou d'impact négatif sur les droits et libertés fondamentales des personnes concernées, lors de la collecte comme de l'analyse.

4.3 Lorsque cela est techniquement faisable, les responsables du traitement des données et, le cas échéant, les sous-traitants devraient tester l'adéquation des 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 le préjudice 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 décrit à la section IV.2.

4.4 En ce qui concerne l'utilisation des données sensibles, des solutions dès la conception doivent être adoptées de manière à éviter, tant que faire se peut, 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.

4.5 Les mesures de pseudonymisation, qui ne dispensent pas de l'application des principes pertinents de protection des données, peuvent réduire les risques pour les personnes concernées.

5. Consentement

5.1 Le consentement libre, spécifique, éclairé et non-équivoque doit se fonder sur les informations communiquées à la personne concernée conformément au principe de transparence du traitement. Compte tenu de la complexité de l'utilisation des mégadonnées, ces informations doivent comprendre les résultats du processus d'évaluation des risques décrit à la section IV.2 et pourraient également être communiquées 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, les responsables du traitement et, le cas échéant, les sous-traitants doivent fournir aux personnes concernées

des moyens techniques accessibles et d'utilisation facile leur permettant de réagir à tout traitement de données incompatible avec les finalités initiales et de retirer leur consentement.

5.3 Le consentement n'est pas donné librement en cas de déséquilibre manifeste des pouvoirs entre la personne concernée et le responsable du traitement ; déséquilibre de nature à influer sur les décisions de la personne concernée à l'égard du traitement. Le responsable du traitement devrait démontrer que ce déséquilibre n'existe pas ou qu'il est sans incidence sur le consentement donné par la personne concernée.

6. Anonymisation

6.1 Les principes de protection des données sont à appliquer dès lors que les données permettent l'identification ou la ré-identification des personnes.

6.2 Le responsable du traitement devrait évaluer le risque de ré-identification en tenant compte des délais, efforts ou ressources nécessaires au regard de la nature des données, du contexte de leur utilisation, des techniques de ré-indentification disponibles et des coûts correspondant. Les responsables du traitement devraient démontrer l'adéquation des mesures d'anonymisation des données et garantir l'efficacité de la dé-identification.

6.3 Les mesures techniques peuvent être combinées avec des obligations juridiques ou contractuelles afin de prévenir toute ré-identification possible des personnes concernées.

6.4 Les responsables du traitement doivent réévaluer régulièrement le risque de ré-identification, eu égard aux avancées technologiques relatives aux techniques d'anonymisation.

7. Rôle de l'intervention humaine dans les prises de décision reposant sur les mégadonnées

7.1 L'utilisation de mégadonnées devrait préserver l'autonomie de l'intervention humaine 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 fortement atteinte aux droits individuels ou de produire des effets juridiques, un décideur (personne physique) devrait, à la demande de la personne concernée, l'informer du raisonnement qui sous-tend le traitement de données, y compris les conséquences de ce raisonnement pour la personne concernée.

7.4 Sur la base d'arguments raisonnables, le décideur (personne physique) devrait se voir conférer la liberté de ne pas se baser sur les résultats des recommandations découlant de l'utilisation des mégadonnées.

7.5 En présence d'indications permettant de penser qu'il y a eu discrimination directe ou indirecte fondée sur les analyses résultant des mégadonnées, les responsables du traitement 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. *Open data*

8.1 Compte tenu de la disponibilité des outils d'analyse de mégadonnées, les entités publiques ou privées, devraient examiner minutieusement leurs politiques d'ouverture (*open data*) des données en ce qui concerne les données à caractère personnel, notant que l'*open data* peut être utilisée afin de formuler des déductions au sujet de personnes ou de groupes.

8.2 Lorsque des responsables du traitement adoptent une politique d'open data, le processus d'évaluation décrit à la section IV.2 devrait prendre en considération les effets de la fusion et de l'exploration de données

relevant de différents ensembles de données ouvertes, également à la lumière des dispositions visées au paragraphe 6.

9. Éducation

Pour aider les personnes 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 de l'information et du numérique comme un élément essentiel de l'éducation.

Les méga données (*Big data*) changent notre façon de comprendre la société. Elles révèlent des perspectives nouvelles et offrent des opportunités en matière d'innovation, d'amélioration de la productivité et de participation sociale.

Les Lignes directrices visent les mégadonnées qui reposent sur le traitement de données à caractère personnel. Elles sont destinées à aider les décideurs politiques et les entités qui traitent ces données, en vue de garantir que les personnes restent au centre de nos économies digitales et que leurs droits et libertés fondamentales soient respectés.

La nature même des méga données peut influer sur l'application des principes traditionnels de protection des données, tel que le principe de finalité ou de minimisation des données. Les Lignes directrices visent à offrir des garanties aux personnes concernées. Il est notamment primordial d'assurer que l'autonomie personnelle et le droit de contrôler ses données personnelles soient garantis et que chacun puisse en jouir dans un contexte de méga données.

PREMS 013517

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont les 28 membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en oeuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE