



Résolution sur les mégadonnées

Auteur

- Autorité de protection des données – Norvège

Co-auteurs

- Autorité de protection des données – Pays-Bas
- Commissariat fédéral à la protection des données et à la liberté d'information – Allemagne
- Préposé fédéral à la protection des données et à la transparence – Suisse
- Bureau de l'ombudsman chargé de la protection des données – Finlande
- Autorité de protection de données – Italie
- Commissariat à l'information – Royaume-Uni
- Bureau d'inspection de la protection des données – Estonie
- Agence de protection des données – Danemark
- Agence de protection des données – Suède
- Commissariat à la protection de la vie privée – Canada
- Commissaire à la protection des données – Berlin
- Agence de protection des données – Espagne

On affirme régulièrement que la capacité de stocker et d'analyser de grandes quantités de données présente des avantages pour la société. Par exemple, les mégadonnées peuvent aider à prévoir la propagation d'épidémies, à mettre au jour les effets secondaires graves des médicaments et à combattre la pollution dans les grandes villes. Certaines utilisations ne nécessitent pas le recours à des renseignements personnels. Cependant, les mégadonnées peuvent également être utilisées à des fins qui suscitent de grandes préoccupations quant au respect de la vie privée des intéressés et à la protection des droits civils et elles pourraient donner lieu à des résultats discriminatoires et porter atteinte au droit à un traitement égal.

Les mégadonnées supposent une nouvelle façon d'examiner les données et révèlent de l'information qu'il était peut-être difficile d'extraire auparavant ou qui, sinon, était cachée. Dans une large mesure, les mégadonnées donnent lieu à une réutilisation des données. La valeur des données peut être liée à la capacité de prévoir des actions ou des événements *futurs* qui y est associée. Les mégadonnées peuvent donner l'impression qu'elles remettent en question les principes clés de protection des données personnelles, plus particulièrement les principes de limitation des fins et de limitation des données.

La protection assurée en vertu de ces principes est plus importante que jamais à une époque où l'on recueille une quantité croissante de renseignements à notre sujet. Les principes de protection des données personnelles servent de fondement aux mesures de sécurité contre un profilage exhaustif dans un éventail sans cesse croissant de nouveaux

contextes. Un affaiblissement des principes clés de protection des données, combiné avec une utilisation accrue des mégadonnées, portera vraisemblablement atteinte à la vie privée et à d'autres droits fondamentaux.

Les membres de la Conférence internationale et d'autres intervenants, dont le Groupe de travail international sur la protection des données dans les télécommunications (IWGDPT, aussi appelé « Groupe de Berlin ») se sont penchés sur la protection des données et de la vie privée en lien avec les mégadonnées. Dans la Déclaration sur le profilage adoptée en 2012 en Uruguay et la Résolution sur le profilage adoptée en 2013 à Varsovie, la Conférence internationale a soulevé des préoccupations concernant la protection de la vie privée. Afin d'encourager davantage les efforts visant à réduire les risques associés à l'utilisation des mégadonnées,

la 36^e Conférence internationale des commissaires à la protection des données et de la vie privée exhorte toutes les parties qui utilisent les mégadonnées à faire ce qui suit :

- Respecter le principe de détermination des fins.
- Limiter la quantité de données recueillies et stockées à celles qui sont nécessaires pour réaliser la fin licite prévue.
- Obtenir, s'il y a lieu, un consentement valide des intéressés à l'utilisation de leurs renseignements personnels à des fins d'analyse et de profilage.
- Faire preuve de transparence concernant les données qui seront recueillies, leur traitement et les fins auxquelles elles serviront ainsi que la question de savoir si elles seront communiquées ou non à des tiers.
- Veiller à ce que les individus aient un accès approprié aux données recueillies à leur sujet ainsi qu'à l'information et aux décisions les concernant. En outre, ils devraient être informés de la source des diverses données personnelles et, s'il y a lieu, pouvoir corriger les données se rapportant à eux et avoir à leur disposition des outils efficaces pour contrôler ces données.
- Veiller à ce que les individus aient accès, s'il y a lieu, aux principaux intrants et aux critères décisionnels (algorithmes) à la base de l'établissement d'un profil. Dans les cas où ces renseignements sont fournis, ils devraient être présentés dans un format clair et compréhensible.
- Mener des évaluations des facteurs relatifs à la vie privée, en particulier lorsque l'analytique des mégadonnées donne lieu à des utilisations nouvelles ou imprévues des renseignements personnels.
- Développer et utiliser des technologies pour les mégadonnées conformément aux principes du *Privacy by Design*.
- Examiner les cas où l'utilisation de données dépersonnalisées améliorerait la protection de la vie privée. La dépersonnalisation peut aider à atténuer les risques d'atteinte à la vie privée associés à l'analyse des mégadonnées, mais uniquement si elle est conçue et gérée de façon appropriée. La solution optimale pour dépersonnaliser des données devrait être déterminée au cas par cas et pourrait faire appel à plusieurs techniques.
- Faire preuve d'une grande prudence avant de communiquer ou de publier des ensembles de données associées à un pseudonyme ou qui peuvent être associées indirectement à un individu par d'autres moyens, et respecter les lois applicables en matière de protection des données. Si les données contiennent suffisamment

de détails qui peuvent être combinés avec d'autres ensembles de données ou qu'elles renferment des renseignements personnels, l'accès devrait être limité et soigneusement contrôlé.

- Démontrer que les décisions concernant l'utilisation des mégadonnées sont équitables, transparentes et responsables. En ce qui concerne l'utilisation des données à des fins de profilage, les profils et les algorithmes sous-jacents devraient tous deux faire l'objet d'une évaluation continue. Il faut effectuer régulièrement des examens pour vérifier si les résultats du profilage sont responsables, équitables et éthiques, et s'ils sont compatibles et proportionnels avec les fins pour lesquelles les profils sont utilisés. On devrait éviter de causer un préjudice à des individus en raison de résultats entièrement automatisés faussement positifs ou négatifs et il devrait toujours être possible d'effectuer une évaluation manuelle des résultats ayant des répercussions importantes sur les individus.