

Utiliser la protection *intégrée de la vie privée* pour innover au moyen des données massives sans compromettre la confidentialité

Sommaire

Les données figurent parmi les actifs les plus précieux d'une entreprise. Elles sont l'oxygène de l'entreprise moderne, et sont générées à une vitesse étonnante : tous les deux jours, nous créons autant de nouvelles données que toutes celles qui ont été créées depuis les débuts de la civilisation jusqu'en 2003. *Tous les deux jours.*

Le terme « données massives » est utilisé pour désigner non seulement les très grands ensembles de données que nous possédons et que nous continuons de créer, mais aussi les technologies et les processus utilisés pour analyser tous ces renseignements et en extraire de la valeur. Il n'est donc pas étonnant que les entreprises, les gouvernements et d'autres organisations souhaitent ardemment exploiter tout le potentiel des données massives. Les progrès rapides observés récemment dans les domaines de la vitesse de traitement des données et des algorithmes analytiques permettent maintenant de traiter de grandes quantités de données structurées et non structurées à très haute vitesse. Nous sommes en mesure d'établir des liens, de repérer des tendances, de prédire des comportements et de personnaliser des interactions à un degré que nous n'aurions jamais cru possible auparavant.

Données massives et risques d'entrave à la vie privée

Nous sommes confrontés à un problème de taille : nos ensembles de données sont si énormes et notre capacité analytique est si avancée que nous pouvons facilement « faire des liens » et des associations entre des éléments d'information qui, en apparence, ne permettent pas d'identifier une personne, mais qui nous fournissent un portrait global d'une personne, de son mode de vie, de ses habitudes de consommation, de ses réseaux sociaux, etc.

Naturellement, notre capacité accrue à obtenir des renseignements personnels grâce à l'analytique des données soulève des inquiétudes quant à l'effet de cette pratique sur le maintien de la confidentialité de ces renseignements. Les protections fondamentales que nous tenions jadis pour acquises sont menacées par la nature même de l'analytique des données massives. Certains croient que notre perception de la confidentialité doit changer et que la protection de la vie privée fait obstacle à l'analytique et aux innovations qu'elle peut permettre.

Or, cette façon de penser qui nous force à choisir entre la protection de la vie privée et l'innovation est une approche périmée à somme nulle. Nous devons trouver une nouvelle solution qui tiendra compte des intérêts et des objectifs de toutes les parties et créera une situation gagnante pour tous.



Protection proactive de la vie privée : protéger les renseignements personnels et favoriser l'innovation

Nous estimons qu'il est tout à fait possible de protéger la vie privée à l'ère des données massives. Nous pouvons le faire tout en utilisant l'analytique des données pour obtenir de nouvelles perspectives et innover afin de faire progresser les entreprises.

Une des méthodes les plus reconnues pour protéger de façon proactive la vie privée est la *protection intégrée de la vie privée*, un cadre conçu à la fin des années 1990 par Ann Cavoukian, Ph. D., commissaire à l'information et à la protection de la vie privée de l'Ontario. Cette approche consiste à intégrer la confidentialité directement aux spécifications conceptuelles des technologies, des pratiques d'affaires et de l'infrastructure en réseau. Elle procure un cadre utile pour toute entreprise qui souhaite innover tout en préservant la vie privée, une forme de « compromis » qui offre le meilleur des deux mondes. La *protection intégrée de la vie privée* repose sur sept principes fondamentaux qui concilient la nécessité d'offrir une protection robuste des données et la volonté de réaliser des innovations fondées sur les données.

Protéger la vie privée et favoriser l'innovation : stratégies à déployer

De nombreuses stratégies sont à la disposition des entreprises qui souhaitent mieux protéger la vie privée tout en menant des activités d'analytique des données.

- **Minimisation des données** : cette stratégie permet d'éliminer efficacement les risques d'entrave à la vie privée dès le début du cycle de vie de l'information. Elle consiste à concevoir dès le début des systèmes d'analytique des données massives dans lesquels *aucun* renseignement permettant d'identifier une personne n'est recueilli à moins qu'un objectif spécifique et impérieux ne le justifie et jusqu'au moment où cet objectif est défini.
- **Anonymisation** : cette stratégie consiste à utiliser un ensemble d'outils ou de techniques pour éliminer d'un ensemble de données tous les renseignements pouvant servir à identifier une personne, que ce soit directement ou indirectement, par des associations avec d'autres ensembles de données. Ces techniques comprennent la suppression ou le masquage des « identifiants directs », par exemple le numéro d'assurance sociale, et la suppression ou la généralisation des « identifiants indirects », par exemple le code postal.
- **Contrôles d'accès par les utilisateurs** : le contrôle de l'accès est le processus par lequel on accorde ou on refuse les demandes spécifiques d'obtention et d'utilisation de l'information et des services de traitement de l'information connexes. Combiné à d'autres principes de sécurité intégrée tels que le droit d'accès minimal, le besoin de connaître, la confiance minimale et la séparation des tâches, le contrôle d'accès est une façon efficace de protéger les renseignements personnels.

Innovation et protection de la vie privée : vous pouvez gagner sur tous les tableaux

Les données massives ne sont pas près de disparaître, mais cela ne veut pas dire de sacrifier la protection de la vie privée ou de cesser d'innover. Grâce à une planification rigoureuse et à l'application de techniques et de principes tels que ceux qui font partie de la *protection intégrée de la vie privée*, les entreprises peuvent utiliser les données pour obtenir l'effet désiré tout en protégeant les renseignements personnels. Il est possible de gagner sur tous les tableaux.

Pour télécharger la version intégrale du rapport *Utiliser la protection intégrée de la vie privée pour innover au moyen des données massives sans compromettre la confidentialité*, veuillez cliquer [ici](#).

