Pour une entreprise soucieuse des données

« In god we trust, all others must bring data » (en Dieu, nous avons confiance ; tous les autres, qu'ils montrent leurs données), une citation attribuée au statisticien américain W. Edwards Deming, souligne l'importance de la mesure statistique et de l'analyse pour vérifier les faits et confirmer leur véracité. Cependant, à mesure que le volume de données croît de façon exponentielle, cela devient de plus en plus difficile au fil du temps.

Bien que l'épidémie d'infox (fake news) soit plus visible sur les réseaux sociaux, les entreprises sont confrontées à un défi similaire en interne. Des données mal utilisées, fausses ou imprécises peuvent entraîner de graves erreurs dans la prise de décision, ainsi que des atteintes à la réputation et jusqu'à des infractions à la législation qui peuvent entraîner de coûteuses amendes.

Depuis l'entrée en vigueur du règlement général sur la protection des données (RGPD), cet aspect est devenu de plus en plus important, car la législation impose aux entreprises de s'assurer qu'elles savent quelles données elles stockent, où elles les stockent et si elles les utilisent d'une manière conforme et sûre.

Contrairement aux infox destinées à influencer l'opinion publique ou à des fins humoristiques, la désinformation n'est pas toujours motivée par une intention malveillante. Dans un contexte professionnel, par exemple, il se peut que les personnes responsables de l'élaboration des analyses aient des données incomplètes, des compétences insuffisantes ou qu'elles aient l'intention de prouver une hypothèse préconçue.

La bonne nouvelle, c'est qu'il est possible de remédier à ces défaillances par une triple approche : modération, gestion et transparence. Et c'est là qu'interviennent les nouveaux rôles du conservateur de données (data curator) et du délégué à la protection des données (data protection officer ou DPO). Tout comme un conservateur de musée qui réussit à trier de la masse d'objets de sa collection et des informations disponibles pour rassembler les bonnes pièces afin de raconter une histoire, il en va de même pour son homologue en charge des données, qui conserve les données pour être un moteur efficace des décisions opérationnelles. Le DPO assure quant à lui la gouvernance et encourage la responsabilité.

À l'ère du RGPD et des entreprises orientées données, le temps est venu pour les organisations d'assumer leur responsabilité vis-à-vis des données qu'elles détiennent et de la façon dont elles les utilisent.

Accroître la transparence

Dans le cadre du RGPD, les entreprises doivent se montrer transparentes sur les données personnelles qu'elles détiennent sur leurs clients, les raisons pour lesquelles elles les détiennent et ce qu'elles en font. Il sera donc crucial pour les organisations de s'assurer que les fichiers de métadonnées sont tenus à jour avec un lignage (cartographie et audit des flux de données) correct des données. En effet, cela permettra aux organisations de répertorier toutes les modifications, en notant quand et comment les données ont été créées et modifiées. Cela sera d'une valeur

inestimable pour renforcer l'intégrité de l'analyse des données en fournissant un historique clair des modifications – permettant de surveiller et de modifier tout changement imprévu.

Cette philosophie se retrouve dans le modèle de fonctionnement de Wikipédia, qui repose sur une collaboration ouverte et transparente, avec des enregistrements transparents des contenus modifiés, par

qui et quand. Le résultat est un service rigoureusement décentralisé qui cherche à fournir une information fiable et équilibrée. Il s'agit d'une philosophie dont les entreprises peuvent s'inspirer dans leurs efforts pour éliminer les parti pris et le cloisonnement au sein de leur organisation, en créant une plateforme neutre et mutualisée de données soigneusement gérées.

Gérer les données de manière responsable

Toutefois, même avec une gestion des données totalement transparente, une surveillance est encore nécessaire pour s'assurer que les modifications apportées s'inscrivent dans les structures et les règles de la société et de son secteur. C'est là qu'un modèle de « gouvernance en libre-service » peut s'avérer crucial, permettant ainsi aux utilisateurs d'ajouter du contenu, de le consommer et de le modifier, mais dans les limites d'un ensemble de règles établies que le conservateur de données peut surveiller.
En d'autres termes, chacun est responsable de l'exactitude des données. Cette philosophie, combinée au référentiel de règles du conservateur de données, garantit que les données restent exactes, identifiées et contrôlées, une démarche essentielle pour la découverte des données ainsi que leur analyse et leur enrichissement.

De même, avec la grande quantité d'informations dont disposent les entreprises aujourd'hui, le potentiel en matière de données peut donner l'impression d'une saturation des données. Avec la décentralisation croissante de l'information au sein des organisations du fait de la multiplication des sources, les employés doivent souvent puiser dans de multiples canaux d'information qui doivent être gérés et rassemblés efficacement avant de pouvoir être utilisés. Le conservateur de données est un élément essentiel de ce processus.

L'obligation imposée par le RGPD à de nombreuses grandes entreprises de nommer un responsable de la protection des données renforce cette fonction dans le tissu des organisations, créant ainsi une figure centrale qui informe et conseille l'organisation sur la conformité en matière de protection des données. Ce personnage central chargé d'assurer la validité permanente de l'utilisation des données est un atout précieux pour les entreprises de toutes tailles qui cherchent à prendre des décisions fiables et concrètes à partir de données. Malheureusement beaucoup d'entreprises semblent encore n'être qu'au stade de la théorie.

Selon une récente étude, plus de la moitié des entreprises interrogées n'ont pas été en mesure de répondre aux demandes d'accès et de portabilité des données dans le délai d'un mois fixé par le RGPD. Dans la pratique, les entreprises n'ont pas un suivi approprié des données personnelles et personne n'a été clairement mandaté pour gérer les processus, établir les bonnes pratiques et fournir les solutions technologiques.

La mise en place d'un DPO peut également transformer le RGPD en un facteur de croissance et un différenciateur concurrentiel. Le DPO mettra en place la stratégie, y compris les processus, travaillera avec le département informatique pour sélectionner les bons outils et réunira tous les travailleurs de la donnée et les utilisateurs métier. Par conséquent, il ou elle s'assurera que l'entreprise a un fort esprit d'appropriation des données.

Cette responsabilité joue le rôle de catalyseur vers un sens commun de la protection des données et un consensus général sur la stratégie de gouvernance des données à mettre en place. La nomination d'un DPO est la première, et probablement la plus importante étape vers une gestion des données gouvernée et responsable.