Rétention des données : mettre fin à la crise

Marqués par les récents évènements en matière de données, ces derniers mois auront été difficiles pour de nombreuses entreprises à l'international. Certaines d'entre elles connues en Europe, en Asie ou encore sur le continent américain, ont dû payer plusieurs millions de dollars d'amende ou ont vu leur réputation entachée. La cause ? Une mauvaise gestion ou protection des données et de la vie privée.

Dotés d'importants moyens, les régulateurs de la donnée n'hésitent plus à prendre des mesures drastiques pour assurer le respect de la réglementation relatives aux données et à la vie privée des citoyens. Si certains organismes ont fait preuve de clémence en raison de la crise sanitaire, d'autres ont tout de même tenu à infliger des amendes pouvant aller jusqu'à plusieurs millions d'euros. Dans les hautes sphères des entreprises multinationales, l'enjeu est alors de pouvoir qualifier, gérer et surtout assurer la conformité des données dont elles disposent afin d'éviter de subir le courroux des institutions de régulation.

La violation de données fait généralement sensation. Mais la réelle portée d'un tel incident reste souvent obscure voire mal comprise par les entreprises. Pourtant, le risque sous-évalué lié à la rétention de donnés suffit à mettre l'entreprise à défaut au niveau réglementaire. L'accumulation de dark data ou la conservation de données personnelles non utilisées sont autant de signes d'une stratégie bancale. Mal conduite ou tout simplement mise au second plan, cette gestion de données inadéquate ouvre la porte aux cybercriminels et leur permet de dérober facilement des données sur un serveur oublié ou mal sécurisé. Une violation de données qui découle de mauvaises pratiques de conservation peut être tout aussi difficile à gérer et coûteuse que les incidents de cybersécurité que nous pouvons régulièrement observer.

Les entreprises ont besoin de clarté sur l'ensemble de leur patrimoine de données pour être sûres de respecter leurs obligations réglementaires. Cependant, sans des outils d'automatisation dédiés à l'application des politiques de classification et de suppression des données, le processus peut s'avérer être extrêmement gourmand en ressources.

Des données difficilement quantifiables

Maintenir des pratiques obsolètes et conserver des quantités astronomiques de données sur des systèmes de stockages toujours plus nombreux - car de plus en plus abordables - font croire à tort aux collaborateurs et aux responsables des données que le stockage en masse est une bonne chose. Malheureusement, cette tendance au stockage compulsif des données par « peur du manque » n'est pas idéale, surtout que les acteurs ne comprennent pas vraiment les données qu'ils stockent et ont rarement une idée concrète de leur valeur. En outre, les données accumulées peuvent avoir d'importantes conséquences, surtout lors de la mise en place de nouvelles réglementations.

Pour de nombreuses industries (comme le secteur bancaire), certaines politiques de conservation de données - notamment en termes de délai de conservation - sont entrées dans les moeurs, si bien que beaucoup d'employés n'y prêtent plus vraiment d'attention. Pourtant, certaines réglementations, comme la RGPD, imposent que les données ne soient conservées que sur une durée nécessaire à leur utilisation première tout en offrant aux individus le droit à leur suppression. Il n'est alors pas

surprenant que les entreprises ne sachent pas très bien ce qu'elles peuvent et doivent conserver (et pendant combien de temps) et choisissent souvent d'ignorer la question, de conserver toutes leurs données et de mettre de côté le risque associé.

L'environnement comprenant les données devenant plus complexe et de plus en plus difficile à gérer et à sécuriser, le risque lié à la rétention des données devient omniprésent. La popularité croissante des environnements hybrides et multi-clouds favorise la duplication des données qui, souvent stockées de façon disparates, peuvent rester inutilisées au sein d'une organisation pendant des années. Cette situation est d'ailleurs exacerbée si la suppression ou la catégorisation de ces données ne sont pas optimales. Celles-ci ont alors tendance à être simplement oubliées et à devenir des dark data . De récentes recherches ont d'ailleurs montré que la moitié des données (52 %) détenues par les entreprises sont aujourd'hui des dark data.

Les dark data représentent davantage de risques qu'elles n'ont de valeur. Des quantités non contrôlées augmentent la probabilité pour les entreprises de devoir faire face à des incidents et par la même occasion d'être en infraction, avec tout ce que cela implique (amende, répercussions sur leur réputation etc.). Dans quelle mesure une entreprise peut-elle alors avoir une réelle visibilité sur ses données ? Comment cela impacte-t-il leur capacité à s'assurer de leur conformité ?

Perspectives et automatisation

Les organisations ont besoin d'une nouvelle approche de la gestion des données et doivent en faire une priorité. Outre la nécessité de procéder à des changements opérationnels et culturels, cette nouvelle stratégie exige également une prise de conscience et un réel engagement pour atténuer efficacement le risque de non-conformité.

Aujourd'hui, chaque chef d'entreprise, membre du conseil d'administration ou chef de service est, à sa manière, le responsable des données de son unité opérationnelle. Par conséquent, chacun doit pouvoir jouer un rôle dans la définition de la stratégie de suppression des données, de résolution des problèmes de gestion ou encore de formation des employés pour qu'ils respectent les politiques de conservation des données.

Dans cet objectif, les entreprises doivent améliorer la visibilité sur leurs données en mettant en place des outils dédiés permettant de les qualifier et de savoir où celles-ci sont stockées. Une fois en place, il leur deviendra plus facile de déterminer quelles sont les données à conserver et celles à supprimer. L'étiquetage des données permis par ce type de solutions aidera également à limiter les erreurs, à apposer une date d'expiration aux données, et par conséquent à améliorer leur gestion. En découlent alors, pour les entreprises, une réduction notoire du risque de non-conformité tout en limitant la production de dark data.

Une gestion minutieuse des données, des politiques claires et des outils de classification et de suppression sont autant d'éléments essentiels au respect de la réglementation en vigueur. Pour que la stratégie de données mise en place soit efficace, une entreprise doit fournir à ses employés la possibilité de comprendre et de contrôler les données qu'ils manipulent à l'aide d'outils et de technologies adaptés. En responsabilisant les acteurs en charge de la gestion de données et en mettant en oeuvre de nouvelles capacités d'automatisation, les entreprises pourront y voir plus clair et assurer un avenir serein dans le paysage réglementaire.