Chapitre 14 - Quels responsabilités le numérique crée-t-il pour les organisations ?

Notions :

- Décrire l'apport des technologies numériques aux relations entre les organisations et les citoyens.
- Définir la notion d'algorithme
- Identifier les enjeux de la chaîne de blocs (blockchain)

1. Comment le RGPD permet-il de contrôler l'utilisation des données personnelles ?

Le Règlement général sur la protection des données (RGPD), entré en vigueur en Europe le 25 mai 2018, vise à renforcer le contrôle des citoyens sur leurs données personnelles.

Voici quelques-uns des principaux principes du RGPD qui permettent aux individus de contrôler leurs données personnelles :

- Droit d'accès : les individus ont le droit de savoir quelles données personnelles les détiennent à leur sujet, comment elles sont utilisées et à qui elles sont divulguées.
- Droit de rectification : nous avons le droit de demander que leurs données personnelles soient exactes et à jour.
- Droit à l'effacement : dans certaines situations, les individus ont le droit de demander que leurs données personnelles soient effacées.
- Droit à la limitation du traitement : dans certains cas, les individus peuvent demander que le traitement de leurs données personnelles soit restreint.
- Droit d'opposition : il y a la possibilité de s'opposer à ce que leurs données personnelles soient traitées à des fins de marketing.

En outre, le RGPD impose aux entreprises et aux organisations de :

- Mettre en place des mesures de sécurité adéquates pour protéger les données personnelles contre le traitement non autorisé ou illégal, la perte accidentelle, la destruction ou les dommages.
- Notifier les autorités de contrôle et les personnes concernées en cas de violation de données.

2. Comment sécuriser les données stratégiques ?

Les données stratégiques sont définies comme « toute information de valeur indispensable à la pérennité de l'organisation » (Mallowan, 2012).

Les données stratégiques sont des informations précieuses pour une entreprise, car elles lui permettent de maintenir son avantage concurrentiel, de protéger sa réputation et de prendre des décisions éclairées. La perte ou la corruption de ces données peut avoir des conséquences désastreuses, telles que des pertes financières importantes, des atteintes à la réputation et des interruptions d'activité.

Pour se protéger, les organisations doivent (sans exhaustivité ni exclusivité) :

- Réaliser un audit des risques cyber.
- Mise en place de contrôles de sécurité (les pare-feu, les systèmes de détection d'intrusion et les solutions de chiffrement.
- Former régulièrement leurs membres à la cybersécurité.
- Lors de la réception d'e-mails, se méfier des pièces jointes, ne pas ouvrir celles provenant de sources inconnues, contacter l'expéditeur par un autre moyen, et ne pas cliquer sur les liens.
- Mettre à jour régulièrement les systèmes d'exploitation.
- Procéder à des sauvegardes externes régulières.
- Chiffrer les données stratégiques en transit et au repos : le chiffrement permet de protéger les données même si elles sont interceptées ou volées.
- Recommander l'utilisation de mots de passe longs, complexes, uniques à chaque collaborateur.

La sécurisation des données stratégiques est un processus continu qui nécessite une vigilance constante de la part des entreprises. En mettant en place une stratégie de sécurité complète et en prenant les mesures de précaution appropriées, les entreprises peuvent réduire le risque de perte ou de corruption de leurs données stratégiques.

3. Vers une nécessaire transparence des outils de traitement numérique et de sécurisation des échanges ?

Les organisations publiques ou privées ont de plus en plus recours à des outils digitaux, dont des algorithmes.

Un algorithme est une suite d'instructions ordonnées et précises permettant de résoudre un problème ou d'accomplir une tâche. Il s'agit d'une description étape par étape d'un processus qui peut être exécuté par un ordinateur ou par une personne.

- La transparence des algorithmes

Si la règle est bien codée dans l'algorithme et si les données fournies par l'usager (ou récupérées, voire contre-vérifiées) par le système d'information de l'administration, la décision (ou le calcul, ou l'action générée) sera adaptée.

Ex. : Dans Parcoursup, le fait de demander l'attribution d'une place dans un internat génère un formulaire destiné à calculer des bourses : les données prises en compte sont le revenu net global, le nombre de frères et de sœurs à charge, et le nombre d'étudiants parmi les membres de la fratrie. À

l'issue du questionnaire, une réponse est attribuée au répondant. Par ailleurs, on comprend aisément que l'ensemble des demandes ne pourrait pas être traité individuellement par un agent désigné : le système ne pourrait plus fonctionner.

Le calcul effectué se révèle exact dans la plupart des situations. Cependant, rien ne garantit que l'algorithme sous-jacent tient bien compte de toutes les informations ou qu'il exprime fidèlement les nouvelles règles de l'administration.

À ce titre, les algorithmes méritent d'être transparents. En cas d'erreur, les conséquences sur les citoyens peuvent être dramatiques et durables. Il est donc nécessaire d'exercer des contrôles. La loi pour une République numérique de 2016 fait entrer dans le débat le principe de transparence pour les algorithmes publics. Trois nouveaux droits sont introduits :

- La mention explicite : c'est l'obligation pour l'administration d'indiquer aux usagers qu'un

algorithme est utilisé, et qu'elles sont leurs droits ;

- Les administrations doivent publier la nature des algorithmes s'ils concernent les particuliers ;
- Tout particulier (usager) concerné doit pouvoir accéder à un ensemble d'informations concernant l'algorithme, son fonctionnement précis et avec la clarté requise. Les données traitées pour son cas doivent également être fournies.

- La blockchain : outil de sécurisation des échanges

La blockchain, technologie sous-jacente aux cryptomonnaies comme le Bitcoin, s'impose de plus en plus comme un outil prometteur pour la sécurisation des échanges dans de nombreux domaines. Son fonctionnement décentralisé, transparent et infalsifiable offre des avantages majeurs en matière de confiance et de traçabilité.

Comment la blockchain sécurise-t-elle les échanges ?

- Registre distribué et infalsifiable : chaque transaction est enregistrée dans un registre partagé et distribué entre tous les participants du réseau. Ce registre est immuable, ce qui signifie qu'il est impossible de modifier ou de supprimer les transactions une fois qu'elles y ont été inscrites. Cela garantit l'intégrité et la véracité des données échangées.
- Cryptographie robuste : la cryptographie permet de garantir la confidentialité des données sensibles tout en authentifiant l'identité des participants aux échanges.
- Transparence et traçabilité : toutes les transactions effectuées sur la blockchain sont visibles par tous les participants du réseau. Cela permet une transparence totale des échanges et facilite la traçabilité des biens et des fonds.