Chapitre 15 Quelles responsabilités le numérique crée-t-il pour les organisations ?

Les transformations numériques offrent aux organisations de nouvelles occasions et peuvent toucher l'ensemble des chaînes de valeurs. Elles transforment les relations entre les citoyens et les organisations. L'exploitation des données personnelles oblige les organisations à respecter le règlement général sur la protection des données (RGPD).

Les données stratégiques de l'organisation constituent un patrimoine qu'il convient de protéger.

L'exploitation des données oblige les administrations à la transparence des algorithmes lorsqu'elles prennent des décisions concernant les individus. Le développement des chaînes de blocs (*blockchains*) modifie la sécurisation des échanges et la médiation des contrats.

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

A. Les principes fondateurs du RGPD

Le RGPD (Règlement général sur la protection des données) est un texte qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne. Il est entré en application le 25 mai 2018.

À l'origine, chaque État membre disposait de son propre outil de protection des données personnelles. Le modèle français prend appui sur la loi Informatique et Libertés de 1978, qui a institué la CNIL. L'adoption du RGPD s'impose donc de fait à l'État français qui charge la CNIL de veiller au respect des nouvelles règles en vigueur.
Le RGPD s'applique désormais dans toute l'Union européenne, mais concerne en réalité toutes les organisations ayant à traiter les données personnelles d'Européens ou de personnes résidant en Europe.

Voici les principes fondateurs du RGPD :

- Les organisations sont tenues de préciser la finalité de la collecte de données.
- Les organisations sont dans l'obligation d'informer leurs utilisateurs des traitements informatiques effectués sur leurs données personnelles.
- Les données ne peuvent être conservées indéfiniment, et la durée de conservation doit correspondre à la finalité visée. Les données non utilisées doivent être supprimées.
- Les droits à l'accès, à la rectification ou à l'effacement des données sont renforcés et les méthodes clairement expliquées par les organisations.
- Les entreprises doivent concevoir leur système de façon à garantir la sécurité des données et avertir les utilisateurs des risques.

- Les organisations doivent être, à tout moment, en mesure de démontrer une utilisation correcte et légale des données personnelles.
- Un DPD (Délégué à la protection des données – *DPO* en anglais) doit être désigné (en interne ou en externe) par chaque entreprise. C'est l'interlocuteur de la CNIL en cas d'incident.
- Des sanctions très sévères sont prévues en cas de manquement : jusqu'à 4% du chiffre d'affaires global.

B. Une sévérité accrue pour contrôler l'utilisation des données personnelles

Avec le RGPD, le montant des sanctions peut s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial.Ces sanctions peuvent être rendues publiques. Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- Prononcer un rappel à l'ordre.
- Enjoindre de mettre le traitement en conformité, y compris sous astreinte.
- Limiter temporairement ou définitivement un traitement.
- Suspendre les flux de données.
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte.
- Prononcer une amende administrative.

De nombreuses entreprises, par exemple Google, ont été sanctionnées par la CNIL.

2. Comment sécuriser les données stratégiques ?

A. Les enjeux de la sécurité des données stratégiques

Les organisations, qu'elles soient publiques ou privées, génèrent, obtiennent, manipulent, traitent des données de nature très différentes.

- ***Les données stratégiques sont définies*** comme « toute information de valeur indispensable à la pérennité de l'organisation » (Mallowan, 2012). Certaines données doivent absolument être protégées contre les fuites, ou au contraire contre les risques d'intrusion.

La maitrise de la sécurité des données stratégiques constitue un levier important pour de nombreuses organisations, car elle permet d'améliorer son image et surtout le degré de confiance que ses clients peuvent lui attribuer, incitant dans la foulée d'autres clients à utiliser ses produits et/ou services.

En revanche, un déficit de sécurité des données stratégiques peut fragiliser les organisations vis-à-vis de ses concurrents (perte de part de marché), de ses clients (fuite des clients actuels, moins de nouveaux clients), de ses partenaires financiers (prime d'assurance plus élevée…), des autorités administratives (amendes imposées par la formation restreinte de la CNIL et publication de la sanction).

Les systèmes d'information des services publics sont également concernés car il en va *a minima* de la crédibilité, et parfois de la sécurité d'êtres humains (par exemple lors des attaques contre les logiciels de l'hôpital universitaire de Brno, en République tchèque, des patients ont dû être renvoyés à leur domicile ; de

même les ordinateurs du réseau de la métropole de Marseille ont été attaqués par un *ransomware* en mars 2020).

B. Les méthodes pour sécuriser les données stratégiques

Les maillons faibles constituent souvent la clé d'entrée des personnes malveillantes souhaitant infiltrer ou attaquer les organisations publiques ou privées afin de récupérer des informations stratégiques.
L'ANSSI (Agence nationale de la sécurité des systèmes d'information) est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Elle formule des recommandations aux entreprises pour qu'elles se protègent mieux contre la cybercriminalité, l'espionnage ou encore le sabotage.

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

- Réaliser un audit des risques cyber en utilisant la méthode EBios.
- 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.
- S'attacher les services de SSII spécialisées.
- Porter plainte en cas d'attaque.
- Recommander l'utilisation de mots de passe longs, complexes, uniques à chaque collaborateur.

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 informatiques destinées à résoudre un ou plusieurs problèmes. Pour l'administration, elle est souvent source de performance. En effet, dans certaines situations (par exemple pour le calcul du droit aux bourses), la somme attribuée ou la décision prise par l'administration dépend d'une vérification automatique de la situation de l'usager, sans intervention humaine.

A. 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.

- ***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 quels 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.

B. La blockchain : outil de sécurisation des échanges

Les données sont potentiellement menacées par de nombreux acteurs (hackers, gouvernements étrangers hostiles…). L'arrivée de technologies permettant la création et la diffusion de cryptomonnaies peutêtre étendue à toute la sphère économique : la *blockchain*.
La *blockchain* est un outil technologique qui permet de stocker et de transmettre les informations de manière fiable, transparente et sécurisée. Elle associe l'horodatage, la cryptographie et de nombreux calculs effectués par des ordinateurs disposant de puissantes cartes graphiques.

- **La totalité des opérations effectuées depuis la création de la chaîne** de blocs est traçable par les utilisateurs. Chacun peut donc vérifier la solidité de la chaîne. La sécurité étant au cœur même de la création des *blockchains*, celles-ci sont utilisées par exemple pour créer et diffuser des monnaies virtuelles, garantir des transactions financières (achat/vente de monnaie, d'actions et d'autres titres) ou gérer des contrats de toute nature.

Correctement utilisée, la *blockchain* s'impose donc comme l'une des technologies les plus pertinentes pour assurer la sécurité des échanges.Il est cependant probable qu'elle ne restera pas unique, car les hackers continuent inlassablement d'arriver à leurs fins et de nouvelles parades doivent sans cesse être trouvées.

1. L'utilisation de la *Blockchain*

L'utilisation de la *blockchain* peut être classée dans trois catégories :

– ***les applications pour effectuer des transferts d'actifs*** : de la monnaie, des votes, des actions… ;
– ***les applications pour assurer une meilleure traçabilité des produits*** et des actifs : des colis, des aliments pour connaître la provenance des produits ;
– ***les applications qui exécutent automatiquement*** les conditions des contrats sans nécessité d'intervention humaine.

Les champs d'exploitation de la *blockchain* sont nombreux : la banque, les assurances, la santé, l'agroalimentaire, la logistique, l'industrie musicale, l'immobilier, le commerce international…