Thème 3 Les organisations et la société

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

Objectif de la séance

- Decrire l'apport des technologies numériques aux relations entre les organisations et les citoyens.

Mots-clés :

- **Algorithme :** ensemble d'opérations devant être suivies dans l'ordre pour résoudre un problème.
- **Chaîne de blocs (*blockchain*) :** technologie de stockage et de transmission d'informations, transparente et sécurisée, fonctionnant sans intermédiaire ni organe de contrôle.
- **Données personnelles :** informations permettant d'identifier une personne (adresse IP, localisation, nom, prénom, numéro de téléphone, âge, sexe, numéro de Sécurité sociale, empreinte digitale, plaque d'immatriculation…).
- **RGPD :** le règlement général sur la protection des données du 25 mai 2018 est un règlement européen qui renforce l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel des utilisateurs.
- **Transparence :** fait de transmettre des informations et de rendre compte d'une activité dans l'objectif d'établir une relation de confiance.

A la fin de ce chapitre j'aurai acquis …

Des connaissances	Des compétences
- Utilisation et protection des données personnelles et stratégiques - Transparence des algorithmes - Chaines de bloc *(blocchain)*	- Analyser les transformations numériques et les opportunités aux organisations - Identifier les enjeux du RGPD pour les organisations et pour les citoyens - Comprendre l'utilité de la transparence des algorithmes

1. Comment les organisations exploitent-elles les données des citoyens ?

Document 1 : Identités numériques et données personnelles

Question 1 : Citer parmi les informations concernant François-Xavier, celles qui relèvent de l'identité déclarative et celles qui relèvent de l'identité agissante.

.

Question 2 : Identifiez le type d'identité qui intéresse les entreprises.

Document 2 : Collecte de données personnelles sur les sites internet

Enseigne de distribution spécialisée dans les matériaux et outillages de construction, Bricoman permet à ses clients d'accéder à ses références/produits grâce à son site Internet. Sur ce dernier, une page est consacrée aux données personnelles recueillies par l'entreprise.

Nature des données personnelles collectées

Les données personnelles que nous sommes susceptibles de collecter lorsque vous naviguez sur le site sont des données :

- nominatives de base, telles que vos noms et prénoms, vos photographies, vos date et lieu de naissance, votre adresse postale, votre adresse e-mail, vos numéros de téléphone ;
- techniques de connexion et de navigation, telles que l'adresse IP de votre terminal, la date et l'heure de votre connexion, les pages visitées, les caractéristiques de votre navigateur (type, langue, etc.), les cookies ;
- de localisation géographique (géolocalisation).

[…] **À quel moment vos données personnelles sont-elles collectées ?**

Vos données personnelles sont susceptibles d'être collectées par Bricoman lorsque vous :

- naviguez sur les pages du site, que vous soyez connecté ou non avec vos identifiants ;
- créez votre compte client (rubrique « Mon compte ») ;
- entrez en contact avec notre enseigne (rubrique « Contact ») ;
- publiez vos commentaires, avis et notes sur nos produits et services ;
- effectuez un achat en ligne.

www.bricoman.fr/donnees-personnelles-et-cookies

Question 3 : Expliquez comment Bricoman détermine vos préférences et habitudes à partir des données collectées sur son site.

Document 3 : La publicité ciblée à la télévision

Afin d'aider les acteurs historiques de l'audiovisuel à faire face à la « révolution numérique » (et notamment à l'arrivée de géants tel Netflix), l'Autorité de la concurrence estime que les pouvoirs publics devraient « desserrer » certaines contraintes réglementaires, par exemple en matière de publicité.
[…]
L'Autorité de la concurrence invite tout particulièrement les pouvoirs publics à autoriser les publicités ciblées à la télévision, « sur le modèle de la publicité sur Internet ». L'autorité indépendante fait valoir que la situation actuelle profite avant tout à Google et Facebook, « qui captent l'essentiel de la croissance très rapide de cette forme de publicité dont l'efficacité est de plus en plus recherchée par les annonceurs ». […] Premièrement, en matière de diffusion hertzienne, les chaînes aimeraient « développer un ciblage publicitaire régionalisé, permettant de compléter un message publicitaire national par un complément d'information local ou régional ou de proposer une offre publicitaire spécifique à la population d'une zone géographique ». […] Deuxièmement, les chaînes se sont dites « très intéressées par les perspectives de développement de publicité ciblée via la diffusion IPTV[1], en utilisant les données personnelles collectées auprès des téléspectateurs par les fournisseurs d'accès Internet ».

1. L'IPTV ou *Internet Protocol Television* permet d'accéder à des canaux de télévision avec Internet.

Xavier Berne, nextinpact.com, 25 février 2019

Question 4 : Expliquez pourquoi l'Autorité de la concurrence estime qu'il est nécessaire de rénover la législation en matière de publicité.

Question 5 : Précisez quelles données personnelles seraient pertinentes pour proposer une publicité ciblée *via* la télévision.

Document 4 : Les courtiers en données

Comme sur n'importe quel marché de matières premières (comme les produits agricoles ou le pétrole), les *data brokers* achètent et revendent des données. Néanmoins, ils se distinguent de leurs homologues courtiers d'autres marchés car ils enrichissent ces données, notamment en les agrégeant pour leur donner du sens, en d'autres termes, les *data brokers* analysent les données afin de regrouper les individus en fonction de certaines caractéristiques.
Cette industrie a été créée pour les besoins du marketing afin de permettre un meilleur ciblage publicitaire.

Par exemple, une entreprise de cannes à pêche préférera acheter plus cher une liste de coordonnées de 10 000 personnes qui pratiquent la pêche plutôt qu'une liste de coordonnées de 100 000 personnes dont on ne sait même pas si elles ont un intérêt pour cette activité. En croisant les historiques d'achats sur plusieurs sites marchands et les recherches sur Google, ces courtiers seront capables de les identifier. Ces informations permettent ainsi aux entreprises de mieux cibler les destinataires de publicités en ligne.

Foucher, 2020

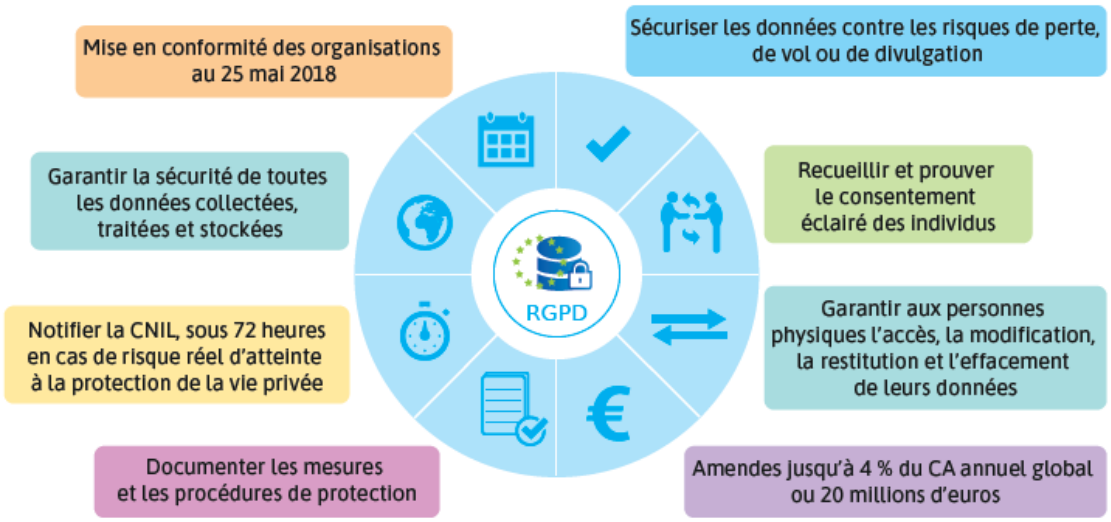
Question 6 : Expliquez le rôle d'un *data broker*.

Question 7 : Montrez l'intérêt de ce métier pour les entreprises

Faites le point sur les notions abordées sur Ma Synthèse de cours
A vous de jouer !

2. Quels sont les enjeux liés à la collecte et utilisation des données ?

Document 1 : Le Règlement générale sur la protection des données applicable depuis mai 2018 (RGPD)



Question 1 : Précisez les types d'organisation visés par ce nouveau règlement.

Question 2 : Comparez les impacts de l'entrée en vigueur du RGPD pour les organisations et pour les utilisateurs d'Internet.

Document 2 : La Loi numérique et transparence des algorithmes au sein des administrations

Aujourd'hui, les algorithmes sont omniprésents. Dans les administrations publiques, de plus en plus de décisions sont prises automatiquement grâce à l'utilisation d'algorithmes plus ou moins complexes : calcul du montant des impôts, attribution d'allocations familiales/de bourses scolaires, accès à l'enseignement supérieur (Parcoursup), etc.
Depuis 2017, la loi Numérique impose à la fonction publique de faire la transparence sur les algorithmes qu'elle utilise pour prendre des décisions individuelles. Pourquoi une telle loi ? Les citoyens doivent être en mesure de comprendre comment sont prises les décisions qui les concernent. Mais est-ce réellement une bonne idée ?

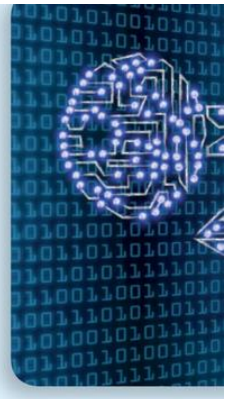
Cette solution ne semble efficace seulement si le citoyen peut comprendre les mécanismes en jeu. La remise en cause des critères ou des hypothèses des algorithmes peut se révéler être un levier démocratique fort pour les citoyens. Grâce à un processus d'apprentissage du fonctionnement des algorithmes, les citoyens peuvent devenir des collaborateurs proactifs et exigeants de l'État. Mais sans accompagnement, on risque de tomber dans un désordre social dont la finalité peut se traduire chez les citoyens par un rejet épidermique de la transformation digitale de l'État.

Foucher, 2020

#vidéo
C'est quoi un algorithme ? - 0,53 min
foucherconnect.fr/20tasdg62

Question 3 : Expliquez pourquoi la loi numérique a rendu obligatoire la transparence des algorithmes pour les administrations publiques.

Coup de pouce ! Comment rendre indispensable la tranparence des algorithmes publics ?



Calculer le montant de votre impôt sur le revenu, attribuer une place en crèche à une famille ou encore gérer l'accès à l'enseignement supérieur : de nombreux services publics sont rendus par l'État et les collectivités, à partir d'algorithmes, de puissants outils parfois décriés pour leur opacité et leur complexité. La loi pour une République numérique (2016) a introduit un principe de transparence de certains algorithmes publics. Comment est-il mis en œuvre ?

Le texte prévoit trois obligations pour les administrations :

1. la mention explicite : c'est-à-dire l'obligation d'indiquer aux intéressés qu'un algorithme est utilisé et quels sont leurs droits ;

2. l'information générale : les administrations doivent publier les principes de fonctionnement des principaux traitements quand ils fondent des décisions administratives individuelles ;

3. l'information individuelle : fournir à l'individu concerné un ensemble d'informations concernant l'algorithme, son fonctionnement en détail et sous forme intelligible ainsi que les données traitées pour son cas spécifique.

Etalab est la mission en charge de l'ouverture et de l'exploitation des données publiques au sein de la direction interministérielle du Numérique. Elle accompagne les administrations dans leur utilisation des algorithmes. Etalab publie un guide sur les algorithmes publics.

Document 3 : Le détournement de données personnelles à des fins politiques

La Federal Trade Commission (FTC[1]) a infligé une amende record de 5 milliards de dollars (près de 4,5 milliards d'euros) à Facebook suite à l'éclatement de l'affaire Cambridge Analytica[2] en mars 2018.

La FTC accuse notamment la société américaine d'utiliser des paramètres « trompeurs » pour les réglages de confidentialité des utilisateurs. « Ces tactiques ont permis à l'entreprise de partager les informations personnelles des utilisateurs avec des applications tierces téléchargées par leurs amis sur Facebook. » [...]

L'amende s'accompagne de mesures obligeant Facebook à mettre en œuvre de « nouvelles protections robustes en matière de confidentialité des utilisateurs. ». La société américaine devra, en outre, mettre en place un comité indépendant sur la protection de la vie privée qui va supprimer « le contrôle absolu » de Mark Zuckerberg, « sur les décisions affectant la vie privée des utilisateurs ».

1. Agence américaine chargée notamment de contrôler les pratiques commerciales.
2. Les données de Facebook avaient été collectées par Cambridge Analytica, afin d'influencer les votes en faveur de Donald Trump lors de la campagne présidentielle de 2016.

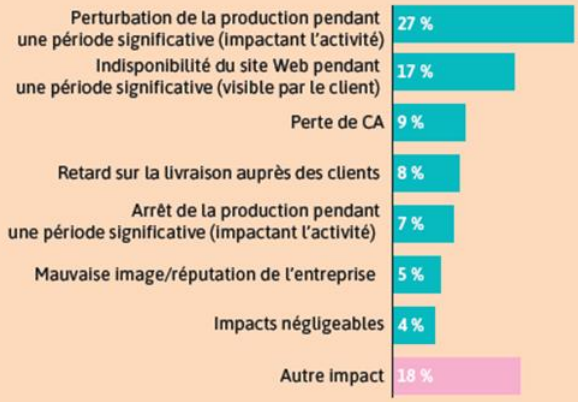
www.generation-nt.com, 24 juillet 2019

Question 4 : Indiquez ce que la FTC reproche à Facebook.

Question 5 : Expliquez quelles ont été les conséquences pour le réseau social.

Document 4 : Les impacts des cyber-attaques en France en 2018

Selon un sondage réalisé auprès de 253 entreprises par OpinionWay pour le CESIN [Club des experts de la sécurité de l'information et du numérique] du 2 décembre 2019 au 7 janvier 2020, 65 % des organisations ont été la cible d'une ou plusieurs cyberattaques au cours des douze derniers mois et près de 57 % d'entre elles déclarent avoir subi un impact négatif sur leur activité.
Près d'une entreprise sur deux se dit inquiète quant à sa capacité à faire face aux cyber-risques. Pour faire face au risque de cyberattaques, les entreprises envisagent notamment d'augmenter le budget sécurité et de mieux former/sensibiliser les usagers aux questions de cybersécurité. Enfin, une entreprise sur deux envisage d'augmenter les effectifs dédiés. Mais la pénurie de profils en sécurité freine les recrutements pour 91 % des répondants.



Sondage OpinionWay pour le CESIN, Baromètre de la cybersécurité des entreprises, janvier 2020

Question 6 : Indiquez pour quelles raisons la protection des données personnelles est importante pour les entreprises.

Question 7 : Relevez les raisons évoquées pour expliquer la vulnérabilité des entreprises vis-à-vis des cyberattaques.

Coup de pouce ! Comment sécuriser ses données stratégiques ?

MENACE	TYPES D'ATTAQUE	COMMENT SE PROTÉGER?
Cybercriminalité	Attaque par hameçonnage (*phishing*) : consiste à usurper l'identité d'un contact connu de la cible et à lui faire faire des manipulations pour obtenir ses informations personnelles.	Se méfier des adresses inconnues. Contacter l'expéditeur par un autre moyen. Ne pas cliquer sur les liens fournis dans l'e-mail.
	Attaque par « rançongiciel » (*ransomware*) : consiste à chiffrer le disque dur de la victime, puis à lui demander une rançon contre déchiffrage.	Se méfier des adresses inconnues. Contacter l'expéditeur par un autre moyen. Procéder à des sauvegardes externes régulières. Mettre à jour son système d'exploitation régulièrement. Déposer plainte en cas d'attaque.
Espionnage	Attaque par point d'eau (*watering hole*) : fait infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour récupérer des données par un malware.	Procéder à des sauvegardes externes régulières. Mettre à jour son système d'exploitation régulièrement. Former les collaborateurs.
	Attaque par hameçonnage ciblé (*spearphishing*) : elle se déroule en plusieurs temps : – Usurpation d'un site officiel ou de l'e-mail d'un proche de la victime. – Contamination par l'ouverture d'une pièce jointe malveillante. – Infiltration du système d'information par la prise de contrôle d'un ordinateur de la victime n° 1. – Obtention des droits d'admin (accès stockage et sécurité). – Vol de données brutal ou progressif en fonction des objectifs. – Effacement des traces.	Procéder à des sauvegardes externes régulières. Mettre à jour son système d'exploitation et ses principaux logiciels régulièrement. En amont : réaliser une analyse des risques cyber en utilisant la méthode EBIOS Risk Manager publiée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). À cet effet, s'attacher les services de SSII spécialisées. Porter plainte auprès de la gendarmerie par la voie classique (si possible demander l'aide d'un gendarme N'Tech).

Sabotage	Fait de rendre inopérant tout ou partie d'un système d'information d'une organisation *via* une attaque informatique.	Informer et former régulièrement les collaborateurs et employés d'une organisation des risques et des actions à mettre en œuvre ou à éviter. Les humains sont souvent le maillon faible d'un système d'information. Utiliser des mots de passe complexes longs et utilisant des caractères spéciaux. Ne jamais donner, transmettre, réutiliser un mot de passe. Ne jamais le placer sur son bureau.

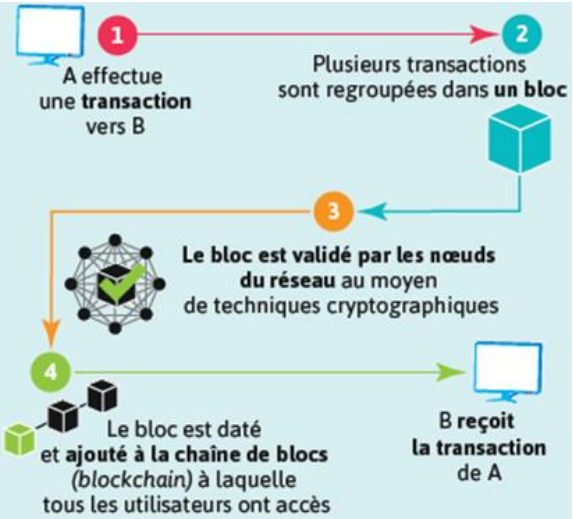
Faites le point sur les notions abordées sur Ma Synthèse de cours
A vous de jouer !

3. En quoi la technologie *Blockchain* vient-elle bouleverser la sécurité numérique ?

Document 1 : Le fonctionnement de la *Blockchain* et ses moyens de sécurité

La ***blockchain*** est une technologie qui permet de garder la trace d'un ensemble de transactions, de manière décentralisée, sécurisée et transparente, sous forme d'une chaîne de blocs. Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé selon des techniques qui dépendent du type de ***blockchain***. Une fois le bloc validé, il est ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau. Ce processus prend un certain temps selon la ***blockchain*** considérée.

#vidéo
Qu'est-ce que la blockchain ?
2,17 min
foucherconnect.fr/20tcsdg63



Question 1 : Expliquez pourquoi le chaînage des blocs et la fréquence de création d'un nouveau bloc sont des moyens de sécurité des données supplémentaires.

Question 2 : Déterminez pourquoi l'accès à tous les utilisateurs est également un moyen de sécurité supplémentaire.

Document 2 : Les impacts de cette nouvelle technologie

Des virements ultra-rapides

La *blockchain*, en permettant d'éliminer les intermédiaires à travers le partage d'une base de données, « a le potentiel pour considérablement changer la manière dont une large gamme de services est exécutée », affirme Colin Ellis, analyste pour l'agence financière Moody's. Aujourd'hui, un virement bancaire entre deux pays nécessite une multitude d'intermédiaires bancaires pour assurer le suivi de la transaction. Avec un registre partagé, l'information pourrait circuler plus rapidement et le nombre d'intermédiaires être limité, permettant de « réduire les coûts opérationnels » d'après M. Ellis. […]

Pressions concurrentielles

Si les banques travaillent sur la *blockchain*, ce n'est pas seulement par opportunisme, mais aussi par nécessité. Selon Anish Mohammed, spécialiste de la *blockchain*, les banques seront confrontées à la pression de nouveaux acteurs, comme en témoigne la multiplication des banques sur Internet et des cryptomonnaies promettant des frais minimes à leurs utilisateurs. Face à cette menace, toutes les banques ne seront pas égales, certaines étant plus dépendantes que d'autres des commissions. C'est le cas des banques suisses (50 % de leurs revenus proviennent des commissions).

AFP, 26 avril 2018

Question 3 : Relevez les avantages que peut retirer le secteur bancaire en utilisant la technologie de la *Blockchain*.

Question 4 : Déterminez pourquoi cette technologie représente également un risque pour ce secteur.

Document 3 : Compatibilité de la technologie *Blockchain et du RGPD*

Question 5 : Expliquez, au vu des contraintes imposées par le RGPD, les risques d'incompatibilité avec la technologie *blockchain*.

Document 3 : Les applications variées de la technologie Blockchain

De nombreux domaines et secteurs d'activité, marchands ou non marchands, publics ou privés, utilisent déjà la *blockchain* ou prévoient de le faire dans les années à venir :

- **dans le secteur de l'assurance,** l'apport de la *blockchain* tient par exemple à l'automatisation des procédures de remboursement et à l'allègement de certaines formalités à la charge des sociétés comme de leurs clients, sous réserve que les hypothèses et les conditions d'indemnisation et de préjudice soient clairement établies ;
- **dans le secteur de la logistique,** la *blockchain* présente deux intérêts : assurer une traçabilité des produits, ainsi que la mémoire des différentes interventions sur une chaîne de production ; alléger les formalités et créer les conditions d'une coopération entre les acteurs d'une filière, notamment en matière d'échange d'informations. […]

Mais de nombreux autres secteurs sont potentiellement concernés par l'utilisation de la technologie *blockchain* : santé, immobilier, luxe, aéronautique, etc.

www.economie.gouv.fr

Question 6 : Expliquez quels sont, globalement, les avantages attendus de la technologie *blockchain* dans les différents secteurs.

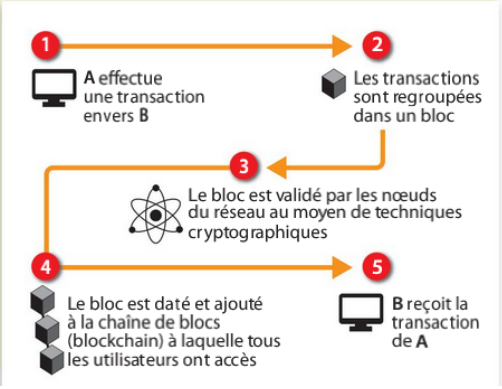
Coup de pouce ! Comment fonctionne la Blockchain ?

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 chaine.

La sécurité étant au cœur même de la création des *blockchains*, elles sont utilisées par exemple pour créer et utiliser des monnaies virtuelles, garantir des transactions financières (achat/vente de monnaie, d'actions et d'autres titres) ou gérer des contrats de toute nature.

Delagrave, 2020.



Faites le point sur les notions abordées sur Ma Synthèse de cours
A vous de jouer !

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

MA SYNTHESE DE COURS

Indiquer les notions abordées dans ce chapitre :

1. Comment les organisations exploitent-elles les données des citoyens ?

2. Quels sont les enjeux liés à la collecte et utilisation des données ?

3. En quoi la technologie *Blockchain* vient-elle bouleverser la sécurité numérique ?