éduSCOL
Informer et accompagner les professionnels de l'éducation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

VOIE TECHNOLOGIQUE

Série STMG : Sciences et technologies du management et de la gestion

2DE | 1RE | TLE

Droit et économie

ENSEIGNEMENT SPÉCIALITÉ

DROIT : LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Mots-clés
Identité numérique – Usurpation d'identité numérique - Données personnelles – Règlement général de la protection des données personnelles – Délégué à la protection des données

La séquence s'articule autour de deux activités qui vont amener les élèves à utiliser plusieurs méthodes :

- l'analyse de documents ;
- l'analyse de faits pour en déduire les qualifications juridiques à utiliser ;
- l'argumentation écrite ;
- et la synthétisation des notions clefs abordées.

Chaque activité est découpée en deux missions :

- la première permet aux élèves de s'approprier les ressources choisies pour développer et acquérir des connaissances en lien avec les notions abordées ;
- la deuxième va conduire les élèves à exploiter la situation donnée en utilisant leurs connaissances et à argumenter sous deux angles différents.

À chaque fin d'activité, il est important de rédiger une synthèse.

La séquence se termine par :

- une question de réflexion qui permet la prise de position par l'élève à l'écrit ;
- une proposition de débat qui permet la prise de position par l'élève à l'oral.

Capacités

Expliquer les enjeux de la protection des données à caractère personnel.

Vérifier le respect des obligations liées à la protection des données à caractère personnel.

Activité 1 - Qu'est-ce que l'identité numérique d'une personne ?

Mots-clés
Identité numérique – Usurpation d'identité numérique

Indication horaire : 2 heures

Outre l'objectif disciplinaire, à savoir définir l'identité numérique, cette activité a pour objectif pédagogique de faire prendre conscience à l'élève que son identité numérique est composée de toutes ses activités sur Internet et que celle-ci doit être protégée.

Situation de travail

Amélia Parker, jeune femme de 35 ans, très active sur internet et plus particulièrement les réseaux sociaux, décide de se présenter aux prochaines élections municipales. Elle crée alors, avec ses amis, un nouveau parti appelé « Maintenant Ensemble ».

Amélia multiplie les actions de communication, notamment par courrier électronique et réunion publique retransmise sur les réseaux sociaux, pour faire connaître ses idées : création de plusieurs festivals culturels et mesures économiques visant à faciliter l'installation de nouveaux commerces (salon de tatouage, traiteur, magasin de jeux en tout genre, …).

Un de ses amis, étonné par le contenu d'un courrier électronique expédié de l'adresse « a_parker_maintenant_ensemble@xxxx.com », l'interroge sur son humour peu ordinaire. En effet, ce mail explique que les deux idées majeures de Amélia ne sont que de la poudre aux yeux et ne verront jamais le jour si elle est élue.

N'étant pas l'expéditrice du courrier reçu par son ami et s'inquiétant pour sa réputation, Amélia vous consulte pour savoir si elle est victime d'une usurpation d'identité numérique.

Vidéo - Identité numérique : C'est quoi ?

Date : mars 2018

Durée : 2'32

Auteur : Staff numérique

URL : https://staffnumeriqueleblog.wordpress.com/2018/03/29/identite-numerique-cest-quoi/

Le QR Code peut être utile dès l'instant où la séquence est travaillée en îlot et que l'enseignant autorise l'usage du téléphone à titre pédagogique.

Doc.1 - Article 226-4-1 du code pénal

« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »

Doc.2 - Procédure en cas d'usurpation d'identité numérique

La procédure classique consiste à se rendre au commissariat ou à la gendarmerie la plus proche. Déposer plainte auprès d'un officier de police judiciaire. Ce dernier va transmettre la plainte au procureur, qui décide de l'engagement ou non des poursuites. D'autres procédures pour porter plainte pour usurpation d'identité numérique sont à votre disposition :

- plainte simple devant le procureur pour usurpation d'identité numérique ;
- plainte avec constitution de partie civile pour usurpation d'identité numérique adressée directement au juge d'instruction ;
- citation directe pour usurpation d'identité numérique, auprès du tribunal compétent, si l'identité de l'auteur de l'usurpation d'identité numérique est connue.

Doc.3 - Usurpation d'identité numérique d'une personne morale

Utiliser le nom de domaine Groupe-Chantelle.com comme adresse de messagerie usurpe l'identité du titulaire de la marque. La commission d'arbitrage et de médiation de l'OMPI en a ainsi décidé le 5 décembre 2016 (Décision OMPI du 5-12-2016, n° D2016-1961, Chantelle S.A. c./ Emmanuel V.).

Les faits sont les suivants. La société de lingerie féminine Chantelle fondée en 1876 est titulaire de plusieurs marques Chantelle ainsi que de noms de domaine composés du radical « GroupeChantelle » utilisés notamment pour ses adresses de messagerie.

Un tiers enregistre le 21 septembre 2016 le nom de domaine Groupe-Chantelle.com. Aucun site web n'est ouvert à partir de ce nom de domaine. En revanche, ce tiers réserve des adresses de messagerie à partir de ce nom de domaine et s'en sert pour adresser des courriers électroniques à des partenaires commerciaux de la société Chantelle en se faisant passer pour de vrais collaborateurs de celle-ci et tenter d'obtenir le paiement de factures sur un prétendu nouveau compte bancaire, prétextant un changement de coordonnées bancaires.

La société Chantelle dépose une plainte auprès du centre d'arbitrage et de médiation de l'Organisation Mondiale de la Propriété Intellectuelle afin de faire cesser ces agissements d'usurpation d'identité en demandant le transfert du nom de domaine Groupe-Chantelle.com à son bénéfice.

Date : février. 2017

Extrait d'un article de maître Alain Bensoussan : auteur : Polyanna Bigle

Source : https://www.alain-bensoussan.com/avocats/usurpation-identite-numerique/2017/02/22/

Mission 1 – Analysez le(s) document(s)

1. Proposez une définition du concept d'identité numérique.
2. Expliquez ce qu'est l'usurpation d'identité.
3. Justifiez le délit d'usurpation d'identité numérique.
4. Indiquez les risques encourus pour avoir usurpé l'identité d'un tiers.
5. Listez les procédures pour porter plainte pour usurpation d'identité numérique en mettant en avant l'élément qui les distingue.
6. Justifiez la possibilité pour une entreprise de déposer plainte pour usurpation d'identité.
   Cette question permet de vérifier le niveau d'acquisition de la capacité « analyser les conséquences de la personnalité juridique » du thème 3.

Mission 2 – Exploitez la/les situation(s) de travail

Il est attendu, ici, que l'élève s'appuie sur le(s) document(s) analysé(s) et ses connaissances pour formuler une réponse argumentée aux questions.

7. Résumez les faits en utilisant des qualifications juridiques
8. Développez l'argumentation que pourrait avancer Amélia pour justifier qu'elle est victime d'une usurpation d'identité numérique.
9. Proposez l'argumentation qui pourrait être opposée à Amélia.
   Les questions 8 et 9 conduisent les élèves à se positionner à la fois du côté d'une partie et à la fois du côté de l'autre.
10. Amélia insiste pour entamer une procédure, conseillez-la en précisant le tribunal compétent.
    Cette question permet de vérifier le niveau d'acquisition de la capacité « sélectionner la juridiction susceptible de juger un litige » du thème 2.

En route vers la synthèse

Il s'agit ici d'amener l'élève à repérer les mots clefs de l'activité et à synthétiser les connaissances acquises afin de développer l'apprentissage par eux-mêmes.

L'identité numérique d'une personne

Listez les mots clefs de l'activité puis rédigez votre paragraphe.

Si le choix est fait d'amener les élèves à réaliser leur propre synthèse, l'enseignant doit, cependant, enrichir leurs travaux par des apports notionnels complémentaires pour répondre aux attentes du programme.

Activité 2 - En quoi consiste la protection des données à caractère personnel ?

Mots-clés
Données personnelles – Règlement général de protection des données personnelles - Délégué à la protection des données

Indication horaire : 1 heure

Outre les objectifs disciplinaires (comprendre les enjeux de la protection des données à caractères personnel, expliquer les obligations imposées par le RGPD et connaître le rôle du délégué à la protection des données), cette activité a pour objectif pédagogique de sensibiliser les élèves sur leur pratique d'Internet, et plus particulièrement aux autorisations qu'ils donnent lors du téléchargement d'application sur leur téléphone, lors de leur navigation sur un site ou un réseau social.

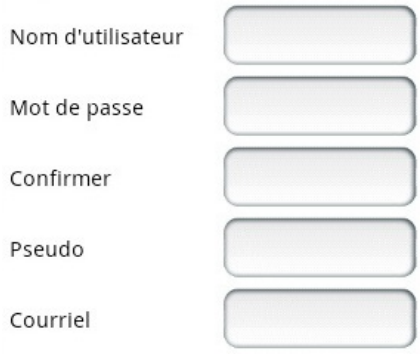
Situation de travail

La société « Aux cafés de Chris », fondée et gérée par Christophe Thompson, fabrique et commercialise des différents produits à base de café (boissons chaudes et froides, desserts en tout genre) dans des « coffee shop » du même nom et situés dans plusieurs grandes villes françaises comme Paris, Lyon, Bordeaux, Nantes, Marseille et à Londres.

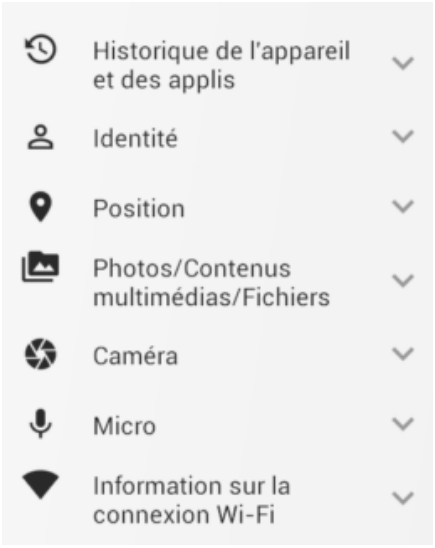
Pour développer son activité, Christophe Thompson investit dans la création d'une application pour ses clients. Cette application pour téléphone, basée sur le principe des réseaux sociaux, nécessite pour accéder au contenu une inscription. Outre les informations collectées au moment de l'inscription, la société peut, à partir des autres informations collectées :

- d'une part affiner la connaissance de son client et vendre les résultats à ses concurrents ;
- d'autre part, envoyer sur le téléphone du client potentiel passant dans un rayon de 5 kilomètres d'un coffee shop « Aux cafés de Chris » une notification contenant un code promotionnel.

Formulaire d'inscription à l'application « Aux cafés de Chris » :



Les accès demandés par l'application au moment du téléchargement :



Vidéo - Données personnelles : les entreprises vous connaissent

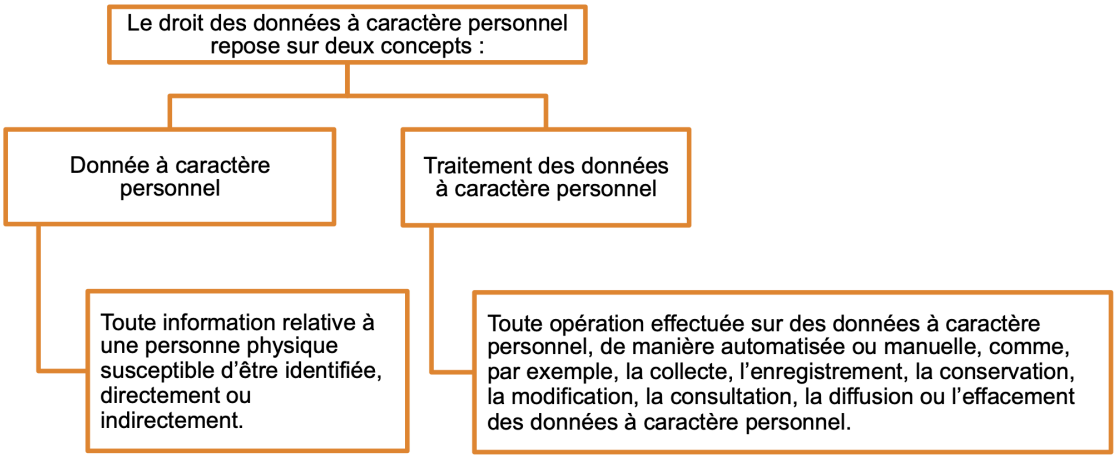
Date : 2018

Durée : 00'57

Auteur : Play Bac Presse/France Télévisions

URL : https://www.youtube.com/watch?v=0Y8bg523LYM

Doc.1 – Le droit des données à caractère personnel



Doc.2 – Les 5 principes du droit des données à caractère personnel

Source : https://www.seban-associes.avocat.fr

Doc.3 – Le règlement général de la protection des données personnelles

Le règlement général de la protection des données personnelles (RGPD) encadre le traitement des données personnelles sur le territoire de l'Union européenne. Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…). Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant. Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

Qui est concerné par le RGPD ?
Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :
- qu'elle est établie sur le territoire de l'Union européenne,
- ou que son activité cible directement des résidents européens.

[…] Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes.

Source : http://www.cnil.fr

Doc.4 – Le délégué à la protection des données

Le responsable de traitement et le sous-traitant doivent désigner un délégué à la protection des données :
- si leur activité fait partie du secteur public ;
- si leur activité principale amène un suivi régulier et systématique de personnes à grande échelle ;
- si leur activité principale amène le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et infractions.

Le délégué est chargé :
- d'informer et de conseiller le responsable de traitement (ou le sous-traitant) et ses employés ;
- de contrôler le respect du règlement européen et du droit français en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être son contact.

[…] Le délégué peut être une personne issue du domaine technique, juridique ou autre.

Source : https://www.service-public.fr

Doc.5 - Les bons réflexes de la protection des données personnelles

Réflexe 1 Pertinence	**Ne collectez que les données vraiment nécessaires** Posez-vous les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?
Réflexe 2 Transparence	**Soyez transparent** Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.
Réflexe 3 Respect des droits	**Pensez aux droits des personnes** Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.
Réflexe 4 Maîtrise	**Gardez la maîtrise des données** Le partage et la circulation des données personnelles doivent être encadrés et contractualisés, afin de leur assurer une protection à tout moment.
Réflexe 5 Gestion des risques	**Identifiez les risques** Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.
Réflexe 6 Sécurité	**Sécurisez vos données** Les mesures de sécurité, informatique, mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

Source : http://www.cnil.fr

Mission 1 – Analysez le(s) document(s)

1. Indiquez si une adresse IP est une donnée personnelle.
2. Expliquez les 5 principes du droit des données à caractère personnel.
3. Justifiez l'élaboration du règlement général de la protection des données personnelles.
   Cette question invite l'élève à réfléchir sur l'évolution de ces dernières années en matière de technologie et permet de vérifier le degré de compréhension de l'articulation entre les normes européennes et nationales abordées dans le thème1.

Mission 2 – Exploitez la/les situation(s) de travail

Il est attendu, ici, que l'élève s'appuie sur le(s) document(s) analysé(s) et ses connaissances pour formuler une réponse argumentée aux questions.

1. Recensez les données personnelles collectées par la société « Aux cafés de Chris ».
   Cette question a pour objectif de faire prendre conscience aux élèves des données qu'ils communiquent bien souvent malgré eux sur Internet et de la nécessité de bien lire avant d'accepter/d'autoriser.
2. Indiquez si la société « Aux cafés de Chris » doit désigner un délégué à la protection des données.
3. Déterminer si le RGPD s'applique pour la clientèle londonienne.
4. Vérifiez si l'application « Aux cafés de Chris » est en conformité avec le règlement général de la protection des données personnelles.

En route vers la synthèse

Il s'agit ici d'amener l'élève à repérer les mots clefs de l'activité et à synthétiser les connaissances acquises afin de développer l'apprentissage par eux-mêmes.

La protection des données à caractère personnel
Lister les mots clefs de l'activité puis rédiger votre paragraphe.

Si le choix est fait d'amener les élèves à réaliser leur propre synthèse, l'enseignant doit, cependant, enrichir leurs travaux par des apports notionnels complémentaires pour répondre aux attentes du programme.

Question de réflexion

L'élève doit, pour cette question, prendre position de manière structurée, en avançant des arguments objectifs.

Faut-il protéger les données numériques à caractère personnel ?

Débat

Notre usage des applications mobiles nous rend-il complice du vol de nos données personnelles ?

Il s'agit d'amener les élèves à formuler, à l'oral, des arguments autour d'une problématique pour laquelle l'enseignant aura pris soin de fournir un ou plusieurs documents support.

Document support

Face aux scandales des données personnelles, un Français sur cinq a quitté un réseau social depuis un an.

À une époque où les scandales de vol de données personnelles se multiplient, avec souvent au cœur de l'affaire un réseau social ou une grande entreprise ; où le Règlement général sur la protection des données (RGPD) est entré en vigueur pour inciter les entreprises du net à plus de vigilance, les internautes du monde entier se montrent de plus en plus méfiants.

L'an dernier, près de 18 millions de Français ont, il est vrai été victimes d'actes de cybercriminalité, pour des pertes estimées à 1,98 milliard d'euros. 67% d'entre eux se déclarent donc plus préoccupés que jamais par le respect de leur vie privée, selon le rapport annuel Norton LifeLock* sur la sécurité en ligne publié ce mercredi. Ils sont par exemple nombreux à réclamer aux entreprises un droit de regard sur l'utilisation qui est faite de leurs données personnelles (97%).

Preuve que les différentes affaires qui ont touché notamment Facebook n'ont pas laissé les Français indifférents, 42% accordent peu de confiance aux réseaux sociaux pour gérer et protéger leurs données personnelles. Et 53% n'en accordent même aucune. Conséquence de ce désamour et des inquiétudes autour de la confidentialité des données, un Français sur cinq (21%) disposant d'un compte sur un réseau social l'a supprimé ces 12 derniers mois.

Et ce sont les plus jeunes qui semblent prendre les choses en main de manière plus radicale. 28% des 18-38 ans ont fermé un compte sur un réseau social contre seulement 15% des 54 ans et plus et 19% des 39-53 ans. […]

Pourtant, assez paradoxalement, c'est dans cette même jeune génération si sensible à la protection des données personnelles que l'on trouve le plus de sondés prêts à partager... leurs informations. Plus d'un jeune de 18 à 38 ans sur deux (52%) se dit même disposé à vendre l'historique de ses recherches internet et 41% sont prêts à laisser filer les informations d'une pièce d'identité. Chez les plus âgés, les chiffres tombent respectivement à 37% pour l'historique et 24% pour les informations sur leur identité.

Et si, malgré quelques réticences, les Français acceptent de partager leurs données, c'est souvent par facilité, souligne le rapport Norton. «Malgré l'envie de mieux protéger leur vie privée et les mesures prises contre les organisations qui gèrent mal les données personnelles, les Français souhaitent que cela soit sans contrainte», note Laurent Heslault, Directeur des Stratégies de Sécurité chez Symantec France, maison-mère de Norton. Ils sont donc prêts à prendre des risques pour des questions de commodité, pour pouvoir utiliser facilement des sites ou services sans avoir à remplir de fastidieux formulaires ou avec des limitations d'usage.

Date : 3 avril 2019

Auteur : Melinda DAVAN-SOULAS

Source : www.lci.fr