

Chapitre 13

QCM

- 1. B.** La qualification de « vol » n'est pas applicable aux données puisque le propriétaire n'en est généralement pas dépossédé et qu'il ne s'agit pas de biens physiques. L'article 323-3 du Code pénal a été modifié le 15 novembre 2014 pour réprimer les faits « d'extraire, de détenir, de reproduire, de transmettre » frauduleusement des données.
- 2. D.** Un logiciel est une œuvre intellectuelle soumise à droits d'auteur et protégée par le Code de la propriété intellectuelle (article L. 122-6-1).
- 3. D.** Dans l'ensemble de l'Union européenne.
- 4. D.** Le non-respect par les entreprises de leurs obligations (consentement, sécurisation) ou interdictions (conservation, traitement, transfert) dans le cadre de traitements automatisés de données personnelles est puni de 300 000 € d'amende et cinq ans d'emprisonnement (respectivement, articles 226-16, 226-17, 226-20, 226-19, 226-22-1 du Code pénal).
- 5. D.** Toute information relative à une personne physique qui peut ainsi être identifiée de manière directe ou indirecte.
- 6. D.** Il faut déposer une demande d'autorisation en cas d'enregistrement de données sensibles.
- 7. A., B. ET C.** La loi Informatique et libertés octroie aux individus les droits d'information (article 32), d'opposition (article 38), d'accès (article 39) et de rectification (article 40) vis-à-vis des traitements automatisés de leurs données personnelles ; le droit de diffusion n'existe pas.
- 8. A. ET B.** Elles peuvent émettre des recommandations et elles ont un pouvoir de sanction.
- 9. C.** Le droit *sui generis* sur les bases de données offre une protection pendant une durée de 15 ans à compter du 1^{er} janvier qui suit l'achèvement de la base de données.
- 10. B.** Le vol d'identité numérique au travers de la captation de données est sanctionné par l'article 226-4-1 du Code pénal.
- 11. B. ET D.** Le RGPD vise à renforcer les mesures de protection des personnes physiques, notamment sur les traitements qui peuvent être mis en œuvre sur leurs données à caractère personnel. Comme cela n'était pas suffisant, le législateur a introduit la notion de régulation de ces données au sein de l'Union européenne. C'est une obligation pour les organisations de l'UE de veiller à cela.
- 12. A. ET C.** Un hypermarché a l'obligation de veiller à la sécurité de ses clients et il peut donc avoir recours à un système de vidéosurveillance. Mais le système ne doit pas être utilisé pour s'assurer que le personnel fait correctement son travail.
- 13. B. ET C.** Le numéro de sécurité sociale est bien une donnée à caractère personnel car il identifie une personne physique : il est unique et spécifique à chaque individu. Il en est de même qu'une photographie d'identité car celle-ci permet d'identifier une personne physique.
- 14. A.** Les informations recueillies à travers les cookies ne peuvent être conservées que pour

une durée limitée par les organisations de 13 mois maximum.

15. A, B. ET D. Les organisations collectent des données à caractère personnel dans tout type de situations : cela commence dès le processus de recrutement et se poursuit au cours de l'exécution du contrat de travail, avec un système de vidéosurveillance ou de géolocalisation des salariés par exemple, ou encore au travers du SIRH, lors du traitement des frais de déplacement par exemple.

Exercices

EXERCICE 1 – LES RECOMMANDATIONS D'AXECONSEIL

1. Récapitulez les principaux devoirs des entreprises en matière d'utilisation des données à caractère personnel.

Les principaux devoirs des entreprises fixés par la loi Informatique et libertés sont :

- l'information et l'obtention du consentement de la personne concernée préalablement au traitement de ses données personnelles, qui jouit en outre d'un droit d'opposition à ce traitement pour motifs légitimes, d'un droit d'accès aux données collectées et de rectification de ces données ;
- la sécurisation des données collectées, notamment leur protection contre la modification ou la destruction et la préservation de leur confidentialité ;
- la limitation de conservation des données à la durée stricte du traitement ;
- l'interdiction (sauf exception) de traiter des données sensibles ou liées à des infractions/condamnations pénales de la personne concernée ;
- l'interdiction (sauf exception) de transférer des données personnelles vers un pays hors Union européenne n'assurant pas un niveau suffisant de sécurité des données.

Selon le type de traitement visé, l'entreprise devra formuler préalablement une demande à la CNIL. Tout manquement à ces obligations ou interdictions est passible de sanctions.

2. Expliquez le rôle de la CNIL.

La Commission nationale de l'informatique et des libertés (CNIL) a été instituée par la loi Informatique et libertés du 6 janvier 1978 pour assurer la protection des données personnelles et de la vie privée des individus. Dans ce cadre, elle informe et protège les particuliers et professionnels, et répond à leurs demandes, émet des avis sur des projets de loi ou de décret, vérifie la bonne application de la loi par les entreprises en contrôlant leurs traitements informatiques, prononce des sanctions en cas de manquement, et pratique une veille sur les nouvelles technologies pouvant avoir un impact sur la vie privée.

3. Analysez les risques sociétaux liés au téléchargement illégal de fichiers numériques.

Le téléchargement illégal de fichiers numériques pose la double question :

- de la propriété intellectuelle : la multiplication des possibilités de partage de contenus sur Internet (sites, réseaux P2P, blogs, etc.) conduit à une remise en cause généralisée du droit d'auteur ; elle induit un manque à gagner, notamment financier, pour les créateurs de contenus

CORRIGÉ

qui ne peuvent plus récolter les fruits de leurs efforts, les industries investissent moins en R&D, etc. ; si ces pratiques se développent, certaines industries finiront par ne plus se renouveler, notamment les industries culturelles : par exemple, le téléchargement illégal de fichiers musicaux entrave déjà l'industrie musicale ; le partage de fichiers vidéo menace l'industrie du cinéma ; il en est de même pour l'industrie du livre, du jeu vidéo, etc. ; le modèle juridico-économique actuel tout entier est remis en cause ;

- de l'éthique dans notre société : de nombreux utilisateurs avouent enfreindre régulièrement certaines lois qu'ils perçoivent comme « de moindre importance » ; ces pratiques, de plus en plus courantes, sont dangereuses parce qu'elles répandent dans l'opinion publique non seulement l'idée d'une culture gratuite, mais aussi la possibilité de commettre des infractions massives sans être sanctionné ; ce phénomène dépasse malheureusement les frontières françaises.

EXERCICE 2 – MISE EN PLACE DE LA GED

1. L'entreprise doit-elle déclarer un nouveau traitement à la CNIL ?

Les opérations de dématérialisation et d'indexation des documents papiers évoquées :

- constituent un seul traitement puisqu'elles sont réalisées en vue d'une même finalité ;
- concernent des pièces se rattachant à un ou plusieurs traitements d'ores et déjà réalisés, donc normalement déclarés par l'entreprise à la CNIL (notamment responsable du traitement, des données collectées, des personnes habilitées à y accéder, de la durée de conservation, etc.).

Ces opérations ne doivent donc pas faire l'objet d'une nouvelle déclaration à la CNIL.

2. Quels changements substantiels la GED peut-elle introduire dans les traitements réalisés, et que doit faire l'entreprise le cas échéant ?

La mise en place d'une gestion électronique des documents peut parfois entraîner la modification de certaines caractéristiques substantielles des traitements déjà réalisés, comme par exemple la durée de conservation des données, le responsable du traitement, les mesures de sécurité en place, etc. Le cas échéant, ces modifications substantielles devront être intégrées dans la formalité initialement réalisée auprès de la CNIL, pour actualisation.

3. Les données sont conservées dans le *cloud*. L'entreprise peut-elle conserver ces données de manière définitive ?

Il faut d'abord analyser le type de données stockées. S'il s'agit de données à caractère personnel, leur conservation est limitée dans le temps.

Il s'agit d'un principe général énoncé à l'article 5 du RGPD, qui impose à chaque responsable de traitement de déterminer une durée de conservation des données personnelles cohérente et justifiée au regard de l'objectif de leur traitement. Une organisation ne peut donc pas conserver des données personnelles de manière illimitée, sauf dans certains cas spécifiques et limités à ce qui est strictement nécessaire.

EXERCICE 3 – RÉGLEMENTATION ET LOGICIELS

1. Que dit la loi concernant les logiciels ?

Un logiciel est considéré comme une œuvre intellectuelle soumise au droit d'auteur. Il appartient à son créateur. Si le créateur est indépendant, il est titulaire du droit de propriété. Si le logiciel est créé par un employé, c'est l'employeur qui en est le propriétaire.

CORRIGÉ

2. A-t-on le droit de faire une copie d'un logiciel ?

Les droits de reproduction d'un logiciel sont encadrés par la loi. La copie d'un logiciel est autorisée pour en faire une sauvegarde ou pour étudier le fonctionnement du logiciel. Un logiciel est protégé par le Code de la propriété intellectuelle.

3. Le nombre de licences achetées par l'organisme de formation est-il suffisant ?

Non, le nombre de licences achetées par l'organisme de formation n'est pas suffisant. Le nombre d'installations sur poste informatique du logiciel de gestion intégré doit obligatoirement correspondre au nombre de licences achetées.

Cas de synthèse

ANALYSER LES DONNÉES À CARACTÈRE PERSONNEL TRAITÉES PAR UNE ENTREPRISE DANS LE CADRE DE SON ACTIVITÉ

Mission 1 :

1.1. L'entreprise a collecté les données de ses clients pour les livraisons. En a-t-elle le droit ?

Ici, les données collectées pour les livraisons sont des données à caractère personnel puisqu'il s'agit des noms et adresses des clients, ainsi que de leurs coordonnées téléphoniques. Le règlement européen de protection des données à caractère personnel (RGPD), entré en vigueur en 2018, est venu renforcer la protection des données instituée par la loi Informatique et libertés du 6 janvier 1978. Pour collecter les données de ses clients, l'entreprise doit, au préalable, non seulement recueillir leur consentement, mais également tenir un registre de traitement de ces données.

1.2. Les clients ont-ils un droit de regard sur leurs données à caractère personnel ?

Oui, les clients bénéficient d'un droit de regard sur leurs données à caractère personnel. La loi Informatique et libertés du 6 janvier 1978 garantit le respect d'un certain nombre de droits pour les clients de cette société. Ils pourront notamment être informés des traitements, accéder à leurs données, exercer leur droit de rectification, s'opposer à l'utilisation de leurs données ou exercer leur droit à l'oubli.

1.3. Pendant combien de temps l'entreprise peut-elle conserver les données de ses clients ?

La durée de conservation des données est limitée dans le temps, afin d'éviter l'accumulation de données. Elle doit être la plus courte possible selon l'article 6 alinéa 5 de la loi Informatique et libertés (la conservation des données est limitée à « une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »).

CORRIGÉ

Mission 2 :

2.1. Dans un mail adressé au dirigeant, rappeler les conditions générales de vente applicables au site Internet de la société pour être en conformité avec le RGPD et les différents textes.

Le site Internet de la société doit respecter le Règlement général de protection des données (RGPD) et la loi Informatique et libertés du 6 janvier 1978, notamment les points de vigilance suivants :

- recueillir préalablement à la collecte des données le consentement libre et éclairé des personnes concernées ;
- informer les utilisateurs du site sur leurs droits concernant la collecte et le traitement de leurs données ;
- respecter la confidentialité et une durée limitée de conservation.

De plus, les points de vigilance ci-dessus ne s'appliquent pas uniquement aux fichiers, mais également aux cookies (traceurs). La CNIL rappelle en effet que « *les internautes doivent être informés et donner leur consentement préalablement à l'insertion de traceurs* ».