IUT DUT INFORMATIQUE - DROIT DES TIC
2018/2019

LA PROTECTION DES DONNEES PERSONNELLES

« L'INFORMATIQUE DOIT ÊTRE AU SERVICE DE CHAQUE CITOYEN. ELLE NE DOIT PORTER ATTEINTE NI À L'IDENTITÉ HUMAINE, NI AUX DROITS DE L'HOMME, NI À LA VIE PRIVÉE, NI AUX LIBERTÉS INDIVIDUELLES OU PUBLIQUES.

TOUTE PERSONNE DISPOSE DU DROIT DE DÉCIDER ET DE CONTRÔLER LES USAGES QUI SONT FAITS DES DONNÉES À CARACTÈRE PERSONNEL LA CONCERNANT, DANS LES CONDITIONS FIXÉES PAR LA PRÉSENTE LOI ».

Loi n° 78-17 du 6 janvier 1978, Article 1er

LA PROTECTION DES DONNEES PERSONNELLES

1. CADRE LÉGISLATIF ET INSTITUTIONNEL

LE CADRE LÉGISLATIF

- Article 9 du code civil (France)
- Article 8 de la Convention Européenne des Droits de l'Homme (Conseil de l'Europe)
- Loi informatique et liberté du 6 janvier 1978 - modification en cours (France)
- Convention 108 du 21 janvier 1981 (Conseil de l'Europe)
- Directive 95/46/CE relative à la protection des données à caractère personnel et à la libre circulation de ces données (Union Européenne)
- Article 7 et 8 de la Charte des droits fondamentaux du 18 décembre 2000 (Union Européenne)
- Directive 2001/31/CE Commerce électronique (Union Européenne)
- Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Union Européenne)
- Règlement Général Sur la Protection des Données du 14 avril 2016 (Union Européenne)
- Loi pour une République numérique du 7 octobre 2016 (France)
- Règlement E-privacy - fin 2019 ? (Union Européenne)
- Les avis et recommandations de la CNIL, du G29 et du Conseil de l'Europe

L'AUTORITÉ DE CONTRÔLE

- La Commission Nationale Informatique et Libertés
- Autorité Administrative Indépendante créée en 1978
- missions : informer, protéger, accompagner, conseiller, contrôler, sanctionner, anticiper
- 200 salariés, 18 commissaires
- budget annuel 2017 : 17 millions, dont 14 millions en personnel
- sanctions prononcées en 2016 : 13, dont 4 sanctions pécuniaires
- nombre de plaintes en 2016 : 7703
- nombre de mise en demeure en 2016 : 82

2. LES NOTIONS CLÉS

LA DONNEE A CARACTERE PERSONNEL

- Informations relatives à une personne physique identifiée ou identifiable. Il s'agit d'informations relatives à un individu dont l'identité est manifeste ou peut être établie à l'aide d'informations complémentaires

- La notion de données nominatives est dynamique et ne s'arrête pas à une liste prédéfinie. Pour savoir si une donnée est à caractère personnel, il faut s'interroger sur le point de savoir si elle est susceptible de permettre directement ou indirectement l'identification d'une personne.

LA DONNEE A CARACTERE PERSONNEL

- Les critères de qualification :
  - une personne identifiée : il est possible de reconnaître individuellement la personne (ex : nom, date et lieu de naissance, ou encore fonction occupée pour les personnes publiques…)
  - une personne identifiable : l'information contient des éléments d'identification permettant de reconnaître directement ou indirectement la personne (ex : l'information du salaire pour un poste particulier) (point 26 du préambule RGPD)
  - la forme des données est indifférente (ex : un échantillon ADN est une DCP)

LE TRAITEMENT DE DONNÉES

- « constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

- Le texte concerne les traitements automatisés mis en œuvre à l'aide de logiciel, mais également les traitements non automatisés tels que des commentaires ou annotations ajoutés manuellement sur une fiche, que ce soit de manière informatique ou manuscrite.

LA PERSONNE CONCERNEE

- Il s'agit de personnes physiques, même s'il est laissé libre aux Etats membres d'adopter des règles pour protéger les personnes morales

- Les DCP englobent les informations relevant de la vie privée de la personne, mais également celles visant ses activités professionnelles ou sa vie publique

LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

- Le responsable du traitement est, sauf désignation expresse par les dispositions législatives ou règlementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens
- Le sous-traitant est la personne qui traite les données pour le compte du responsable de traitement. Il peut s'agir d'une tâche spécifique ou générale
- Les relations entre responsable et sous-traitant : Le responsable décide de traiter la donnée, tandis que le sous-traitant procède au traitement pour le compte du responsable. Le responsable doit contrôler la mise en oeuvre du traitement
- Le sous-traitant devient responsable s'il utilise les données à ses propres fins

LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

- La responsabilité conjointe du traitement (article 26 RGPD) : Les finalités sont définies conjointement par deux ou plusieurs responsables
- La responsabilité du sous-traitant :
  - le sous-traitant doit démontrer qu'il assure un niveau de protection conforme au RGPD
  - il doit être transparent dans le choix de ses sous-traitants vis-à-vis du responsable du traitement
  - le responsable du traitement et le sous-traitant doivent être liés par un contrat ou un acte juridique qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement (article 28.3 RGPD)

DONNÉES SENSIBLES ET CATÉGORIES DE DONNÉES SPÉCIALES

- Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits (article 9 RGPD)
- L’article 9.2 prévoit plusieurs exceptions à l’interdiction, comme le consentement de la personne
- il est nécessaire de faire un examen de proportionnalité entre l’atteinte raisonnable et/ou justifiée à la vie privée et les besoins du traitement (ex : intervention médicale en urgence alors que la personne n’est pas en état de donner son consentement)

RESTRICTIONS APPORTÉES À L'APPLICATION DES TEXTES

- Sont exclus les traitements sur des domaines ne relevant pas du marché interne de l'UE :
  - sûreté publique, défense, sécurité nationale, application du droit pénal
  - les traitements relevant de la sphère privée
  - peuvent être exclus les traitements par les média
- exemples :
  - caméra de surveillance filmant un lieu privé ne recevant pas du public (pas de violation)
  - publication par une Suédoise d'informations sur les paroissiens fréquentant la même église qu'elle (violation)

3. LES PRINCIPES

LE PRINCIPE DE LICÉITÉ DU TRAITEMENT

- Le traitement est licite s'il :
  - est conforme à la loi
  - poursuit un but légitime
  - la personne a consenti au traitement
  - est nécessaire pour l'exécution d'un contrat, pour le respect d'une obligation légale, pour la sauvegarde des intérêts vitaux de la personne, aux fins des intérêts légitimes ou d'une mission d'intérêt public

LE PRINCIPE DE LICÉITÉ DU TRAITEMENT

Données non sensibles	Données sensibles
consentement	accord explicite de la personne concernée
relation contractuelle prévoyant le traitement	intérêt vital de la personne concernée
intérêt vital de la personne concernée	intérêt légitime d'un tiers (considérants 47 à 50 RGPD)
Intérêt légitime poursuivi par le responsable du traitement ou par un tiers	Intérêt général
mission d'intérêt public ou relevant de l'exercice de l'autorité publique	

LE PRINCIPE DE TRAITEMENT LOYAL ET TRANSPARENT

- Il est nécessaire d'obtenir un consentement explicite de la personne (l'inaction ne vaut pas consentement - principe opt-in)
- la personne concernée doit avoir été informée de la finalité du traitement et de ses droits
- la personne concernée doit connaître l'identité du responsable du traitement
- il est interdit de procéder au traitement secret ou clandestin des données

LE PRINCIPE DE TRAITEMENT LOYAL ET TRANSPARENT

- L'information :
  - collecte réalisée par le responsable : information au plus tard au moment de la collecte
  - collecte réalisée par un tiers : information au plus tard au moment où le responsable enregistre les données ou avant que les données ne soient divulguées à un tiers pour la première fois
- Exceptions à l'obligation d'information :
  - communication impossible
  - l'information exigerait un effort disproportionné
  - l'enregistrement ou la divulgation des données est prévu par la loi

LE PRINCIPE DE LIMITATION DES FINALITÉS

- Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités
- La réutilisation des données est contraire à ce principe
- Le transfert des données à un tiers constitue un nouveau traitement

LE PRINCIPE DE MINIMISATION ET D'EXACTITUDE DES DONNÉES

- Seules les données adéquates et pertinentes peuvent être traitées et uniquement dans la mesure où ce traitement est nécessaire à la réalisation de la finalité invoquée au moment de leur collecte et/ou de leur traitement ultérieur. Les catégories de données choisies en vue du traitement doivent être indispensables pour atteindre le but déclaré général des opérations de traitement
- les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Elles doivent être effacées lorsque ces finalités sont atteintes
- Le responsable du traitement doit s'abstenir d'utiliser les DCP sans prendre de mesure raisonnable visant à assurer leur exactitude et leur mise à jour.

LE PRINCIPE D'INTÉGRITÉ ET CONFIDENTIALITÉ

- Le traitement doit garantir un niveau de sécurité approprié contre :
  - tout traitement illégal ou non autorisé
  - la perte accidentelle
  - la destruction
  - l'endommagement
- Il faut prendre des mesures techniques et organisationnelles adéquates

LE PRINCIPE DE RESPONSABILITÉ

- Le responsable du traitement doit pouvoir rendre compte de la conformité des traitements au droit relatif à la protection des données à caractère personnel :
  - conformité du traitement dès sa conception (article 25 RGPD)
  - mécanisme de notification des violations de sécurité aux APD (articles 33 et 34 RGPD)
  - désignation d'un DPO (ou DPD) ou d'un sous-traitant
  - étude d'impact pour évaluer l'incidence sur la privé des traitement à haut risque (PIA - article 35 RGPD)