

LA COMPÉTENCE DES CPP DANS LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL: RETOUR D'EXPÉRIENCE

Géraldine BOLET, Membre du CPP NO IV

Juriste

NOUVEAU CADRE RÉGLEMENTAIRE
« PROTECTION DES DONNÉES »

LOI INFORMATIQUE ET LIBERTÉS (LIL)/ RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

- **En France**

- Loi informatique et libertés 78-17 du 9 janvier 1978 : Chapitre IX: Recherche
- Loi modifiée par la directive 95/46 CE du 24.10.1995 transposée en France par la loi du 6 aout 2004
- Loi modifiée par la loi de santé du 26 janvier 2016 (fusion chap IX et X)
- Loi n°2018-493 sur la protection des données publiée au JO le 21 juin 2018

- **En Europe**

- Directive 95/46 CE du 24.10.1995
- Règlement Général sur la protection des données à caractère personnel applicable au 25 mai 2018

RGPD



RGPD a pour objectif de:

Unifier la législation européenne sur la protection des données

Renforcement des droits des personnes sur leurs données

Responsabilisation des entreprises/ organismes/ personnes traitant des données à caractère personnel

Les principes de la protection des données:

- Licéité, loyauté et transparence dans l'utilisation des données;
- Limitation des finalités (finalités déterminées, explicites et légitimes);
- Minimisation des données (données adéquates, pertinentes et limitées à ce qui est nécessaire);
- Exactitude des données (données exactes, et tenues à jour);
- Limitation de la conservation (données conservées sous une forme permettant l'identification des personnes pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées);

PRINCIPE D'INTERDICTION DE COLLECTER DES DONNÉES DE SANTÉ

La LIL pose le principe de l'interdiction de collecter des données de santé et le RGPD la maintient

- Art. 8 I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont **relatives à la santé** ou à la vie sexuelle de celles-ci.

Mais

La collecte de données de santé est **exceptionnelle** et **doit être justifié** par soit :

- Le consentement donné par la personne concernée par la collecte
- La **recherche médicale, les études et évaluations dans le domaine de la santé** (*autorisation CNIL / MR + comités d'éthique*)
- La collecte de données de santé est justifié par l'intérêt public / l'intérêt général (*autorisation CNIL*)

DÉFINITIONS (LIL + RGPD)

Responsable de traitement: est la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement

Fichier:

Tout ensemble structuré de données accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Traitement de données:

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Titulaire: Personne habilitée à obtenir la communication de données enregistrées dans un fichier ou un traitement en raison de ses fonctions.

Données à caractère personnel:

Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Données de santé :

Les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

LA NOUVELLE COMPÉTENCE DES CPP

COMPÉTENCE DES CPP

Loi Jardé et décret n°2016-1537 du 16 novembre 2016 relatif aux recherches impliquant la personne humaine

Le **CPP compétent** pour évaluer les données à caractère personnel c'est à dire:

la méthodologie de la recherche au regard des dispositions de la loi informatique et libertés de:

- ❖ la nécessité du recours à la collecte au traitement de données à caractère personnel
- ❖ la pertinence de celles-ci par rapport à l'objectif de la recherche,

préalablement à la saisine de la Commission nationale de l'informatique et des libertés

Mais nouveau cadre réglementaire européen relatif aux données à caractère personnel

CE QUI CHANGE

LOI INFORMATIQUE ET LIBERTÉS

- Protocole conforme à une MR ou Autorisation CNIL
- Information des personnes:
 - Promoteur
 - Finalité du traitement de données à caractère personnel
 - Transfert hors UE
 - Droits
 - Accès
 - Rectification
 - Opposition
 - Coordonnées de la personne pour l'exercice des droits

RGPD (depuis le 25 mai 2018)

- Protocole conforme à une MR ou Autorisation CNIL (après avis du CPP)
- Information des personnes
 - Promoteur
 - Finalité du traitement de données à caractère personnel
 - Transfert hors UE (identification du pays destinataire+ précautions prises par le promoteur)
 - Droits
 - Accès
 - Rectification
 - Opposition / effacement
 - Limitation
 - Droit d'introduire une réclamation auprès de la CNIL
 - Durée de conservation des données
 - Coordonnées du DPO



EXAMEN DES DOSSIERS « PARTIE DONNÉES » PAR LE CPP

Protocole

- Si le promoteur s'est déclaré conforme à une MR : transmission du récépissé de la CNIL
 - MR adéquat (MR001: consentement / MR003: non opposition/ MR002: DM non interventionnelle)
 - les données collectées (pas de données directement identifiantes type photo/vidéo)
 - Transfert hors UE (pays jugés adéquat ou non)
- Si le promoteur ne s'est pas déclaré conforme à une MR:
 - Communication de l'autorisation CNIL après avis du CPP

Lettre d'information / Consentement

- Finalité du traitement (idem f=objectif de la recherche)
- Droits RGPD repris
- Coordonnées pour exercer les droits (boite mail professionnel/ ~~gmail~~/hotmail)
- Durée de conservation des données
- Transfert

POSITION DU CPP NORD OUEST IV

- **Protocole**
- Vérification de la présence d'une MR
 - Si présence d'une MR: communication du récépissé + n° d'enregistrement
 - Détail dans le protocole de la conformité à cette MR
 - Si non mention d'une MR: inscription claire dans le protocole qu'une demande d'autorisation auprès de la CNIL sera faite après obtention de l'avis favorable du CPP
 - Demande du CPP d'obtenir communication de cette autorisation
- Absence totale de mention d'une MR ou recours à une autorisation CNIL
 - Avis suspensif prononcé par le CPP
- **Lettre d'information**
 - Absence des nouveaux droits
 - Avis suspensif

SANCTIONS POUR LES PROMOTEURS

- **Amendes administratives**
- **Niveau 1 (10 M€ ou 2% du CA)** pour les infractions aux dispositions suivantes :
 - traitement ne nécessitant pas l'identification
 - obligation générale du responsable de traitement : registre des activités de traitement, coopération avec la CNIL, sécurité, notification d'une violation de données analyse d'impact, consultation préalable, DPO.
- **Niveau 2 (20M € ou 4% du CA)** pour les infractions aux dispositions suivantes:
 - principe de base d'un traitement
 - licéité
 - consentement
 - catégories particulières de données
 - droits des personnes concernées
 - transferts hors UE
 - liberté d'expression, accès aux documents administratifs, NIR
 - injonction de la CNIL, enquêtes de la CNIL



MERCI POUR VOTRE ATTENTION