Les zones d'ombre

DE LA

LOI INFORMATIQUE ET LIBERTÉS

Par
Frédéric THU

A PROPOS DU CABINET CILEX :

Au service des CIL depuis 2005

CABINET-CILEX.COM

AMBIGUÏTÉS & FLOUS DE LA LIL :

Comment les gérer ?

- **Difficultés** récurrentes face aux textes et **Solutions** pratiques à adopter pour le CIL (30 min.) :
  - **CONCEPTS FLOUS** : traductions, copier-coller hasardeux… imprécisions… : des sources de questionnements
  - **QUELQUES OLNIS** – Objets Législatifs Non Identifiés
  - **TRAVAUX DU CIL**
  - **DIFFICULTÉS PRATIQUES**
- **Échanges,** questions réponses (10 min.)

1.
Concepts flous

- L'**interconnexion** ou le **transfert de données** transfrontalier posent régulièrement question.

- Des concepts classiques censés être clairs :

  - **Donnée à caractère personnel,**
  - **Traitement,**
  - **Destinataire,**
  - **Responsable de traitement…**

- Même « **Sécurité** » évolue depuis quelques années...

CONCEPTS FLOUS

Donnée à caractère personnel

Art. 2 :

« Toute information relative à une personne
identifiée ou **identifiable** »

…et on lit ou entend souvent à tort
*« **donnée identifiante** »*

Donnée à caractère personnel

Sont donc des données à caractère personnel :

- Le montant du salaire
- La liste des achats
- L'IP, même si elle change
- Le gabarit d'empreinte digitale – même isolé, sans information sur les personnes

➡ Le Registre doit comporter ces informations (au moins les catégories),

➡ Le CIL doit diffuser cette définition.

Traitement

Art. 2 :

« Toute **opération** ou ensemble d'opérations portant sur des données à caractère personnel »

Interconnexion ?

*Le WG29 considère qu'écrire ou lire un cookie utilise un **équipement**, et donc **constitue un traitement**.*

CONCEPTS FLOUS

Traitement

La décision « Google » de janvier 2013 se fonde sur ce point pour considérer que Google réalise un traitement en France.

Tout site internet déposant des cookies réalise donc des traitements sur les ordinateurs de ses visiteurs.

L'opérateur d'un site internet de e-commerce français peut dès lors être soumis à d'autres lois :

Loi 09-08 du Maroc, Art.2 :La présente loi s'applique au traitement des données à caractère personnel, automatisé en tout ou en partie,(…), lorsque le responsable n'est pas établi sur le territoire marocain mais recourt, à des fins de traitement des données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire marocain; ce responsable doit notifier à la CNDP l'identité d'un représentant installé au Maroc, se substituant à lui dans tous ses droits et obligations: (art 13) déclaration préalable (amende, art. 52: 100.0000 DH), (art. 18) information aux personnes…
La France est reconnue comme assurant un niveau de protection suffisant depuis le 6 septembre 2013, Délibération 465-2013.

Question: l'implantation et la lecture d'un cookie permettant à un client Vietnamien de ne pas s'authentifier sur un site de commerce est un traitement : est-il soumis à Autorisation de transfert ?

➡ Conséquences pour le CIL : pays tiers, autorisations ?

CONCEPTS FLOUS

Responsable de traitement

Art 3 I :

«…l'organisme qui détermine les **finalités** et les **moyens** »

- La LIL **écarte la co-responsabilité** prévue par la Directive de 1995.
- La LIL ne prévoit pas les **Groupes**.

Le sous-traitant semble être un moyen...
mais détermine souvent les moyens techniques
en dehors d'instructions du Responsable.

*Le Règlement imposera la **co-responsabilité***

CONCEPTS FLOUS

Responsable de traitement

- L'organisme est responsable de tout, il est censé tout contrôler :
  - **CNIL** : Sécurité / Pas de sous-sous traitance / Devenir des données
  - **CILEX** : Auditabilité / Avis en cas de perte de données / contrôle CNIL
- Recours artificiel à la notion de sous-traitant dans les Groupes
- La notion de Groupe est parfois reconnue

  (EADS, 2011-138 : « La société EADS France SAS agit en qualité de responsable de traitement pour l'ensemble des sociétés du groupe EADS concernées par le dispositif d'alerte professionnelle. En effet, la Commission constate qu'elle détermine seule les finalités et les moyens du traitement. »)

CONCEPTS FLOUS

Destinataire

Art 3 II :

«…toute personne habilitée à recevoir communication de ces données, **autre que** :

- la personne concernée,
- le responsable du traitement,
- le sous-traitant,
- et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données,
- non plus que les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer ces données »

➡ *Il n'y a donc plus de **destinataire***

.... Problème de conflit entre le sens commun et le sens légal

CONCEPTS FLOUS

Destinataire

Dans le Registre :

- *« Aucun destinataire en dehors du service gestionnaire »*
- *« Aucun destinataire en dehors des personnes habilitées »*
- *« Service gestionnaire et partenaires commerciaux »*
- *« Service gestionnaire et destinataires légaux »*

La CNIL ne requalifie pas les demandes d'autorisation mal formulées :

AUT 2013-210 : Les personnes destinataires du traitement sont les personnes du service Assurances rattachées à la Délégation générale à la Sécurité Juridique de la Ville de Lyon.

AUT 2013-141 : Les destinataires des données sont les agents spécifiquement habilités, du fait de leurs fonctions, au sein de la direction des affaires juridiques et de la direction de l'insertion et du logement (DIL) du Conseil général du Calvados ; Les données seront communiquées aux autorités compétentes dans le cadre de la procédure pénale.

AUT 2013-120 : Seuls les partenaires de la lutte anti fraude, c'est-à-dire les sociétés FIA NET, CERTEGY (sous-traitants), AUCHAN France et le cabinet de recouvrement « Lucas et Degand », ont accès à ce traitement

CONCEPTS FLOUS

Transfert

1978, 1995 : époque pré-internet, pré-mondialisation…

Pas de définition du **TRANSFERT** ► Interprétation très large

Problèmes :

- Annuaire global AD
- Intranet global
- Agence chinoise via VPN
- DRH sur son PC via VPN
- Ecriture d'un cookie

« *Suffisant* » LIL = « *Adéquat* » D95

CONCEPTS FLOUS

Transfert

Pour le CIL :

- Tous ces cas nécessitent une autorisation de transfert (sauf cookie ?)
- 22 III : le CIL ne dispense pas de déclaration si transfert hors EEE
  (UE + NO, IS, LI)

  Pays à niveau « suffisant » (Canada, NZ, Jersey...) :
  - *en théorie, la formalité est la Déclaration à la CNIL*
  - *en pratique, la CNIL recommande : inscription au Registre*
- Art 69 : les BCR ne dispensent pas d'autorisation de transfert (à chaque nouveau pays…) – même si la décision est accordée automatiquement

CONCEPTS FLOUS

Sécurité

- **Définition classique** : «*Notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* »

- **Évolution récente :** EBIOS (référentiel Label Audit, 2011) :
  « *assurer la confidentialité, l'intégrité et la **disponibilité*** »

  - « *Disponibilité du système de gestion des demandes d'accès, rectification, opposition* » (Guide Sécurité avancé, 06/2012)

- **Évolution récente de la CNIL** : **tracer** les accès afin de détecter les accès non autorisés

  - Mise en demeure Paris Habitat, 2011 : « *L'application XYZ ne comportant pas de mesures de traçabilité des actions, il n'est dès lors pas possible d'identifier a posteriori un accès frauduleux aux données personnelles ni d'en déterminer l'origine ; ces faits constituent un manquement à l'article 34* »

  - Traçabilité des actions : DMP, 2010 ; des modifications d'accès : INSERM, 2011

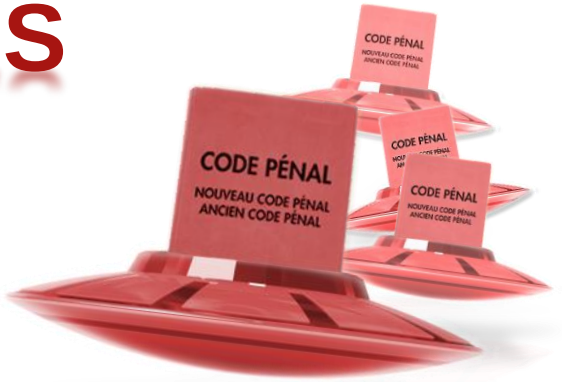
  - Depuis 2012-062, Ville de Paris, la CNIL utilise la formule « *Sur la sécurité des données et la traçabilité des actions* » dans les décisions d'Autorisation.

CONCEPTS FLOUS

Sécurité

- Évaluer la disponibilité ?
- Mettre en place une traçabilité mesurée (éviter le flicage !)
  - Réfléchir en termes de risques pour les personnes
  - Traçables : habilitations, rejets d'accès, accès, modifications spécifiques/ globales, lectures spécifiques/ globales, utilisations anormales (pillage)...
  - Informer les IRP **et** les utilisateurs
  - Déclarer le traitement au Registre
  - Ou demander une Autorisation (traitement détection de fraude)
- Anticiper le Règlement et les notifications de violations de sécurité

2.
Quelques OLNIS



- Registre public
  (art 22: pas de formalité préalable) :
  - Liste électorale, liste d'émargement,
  - Enquête utilité publique,
  - Impôts (*L 111 Livre des procédures fiscales :*
    nom, 1ère lettre du prénom et adresse, nombre de parts retenues pour le calcul du quotient familial, revenu imposable, montant de l'impôt mis à sa charge – consultable par département)

- Déclaration unique (art 23-II)

- Autorisation unique de transfert : permet *1* traitement vers *n* filiales, en dehors de BCR

- Combien d'engagements de conformité pour plusieurs instances de la même classe de traitements (NS/AU) ?

  ➡ **Un seul**

3.

Travaux du CIL

Le registre est-il un traitement ?

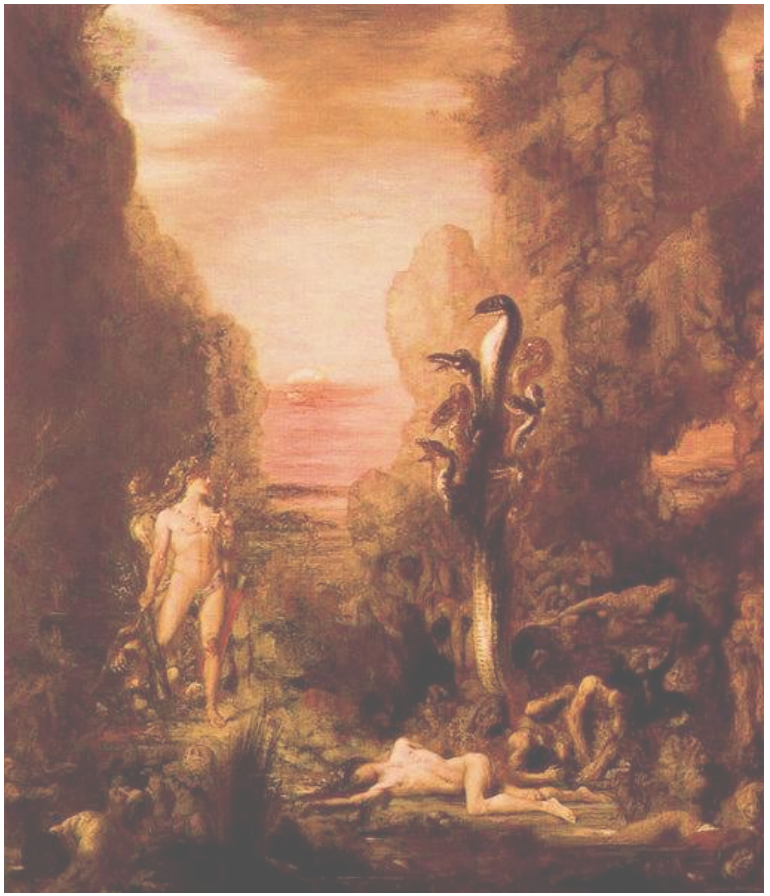
- Non, il ne comporte pas de données à caractère personnel
- Oui, pour l'annuaire du logiciel permettant de le tenir

Bilan : quand le faire ?

- Décret 20/10/2005, art 49, dernier § : « bilan annuel »
- 1 fois par an, de manière régulière
- le premier bilan est souvent décalé (jusqu'à... 36 mois)

Bilan : quel contenu ?

- Recommandations CNIL et AFCDP
- Le Web comporte des Registres publics...
  pas de Bilans



4.

Quelques difficultés pratiques

- Les **fichiers obligatoires** sont-ils soumis à déclaration / autorisation ?
  - les PCA de la grippe H1N1 ont été soumis à déclaration, puis dispensés;
  - 2013-121 Ordre des pédicures-podologues, ou 2013-133 Ordre des Pharmaciens : la gestion des sanctions est soumise à autorisation.
- Propagation du **droit d'opposition** (Décret, art. 99)
- « **il**légalité » des **directions juridiques** : ne sont pas des auxiliaires de justice, donc pas légalement habilitées à traiter des informations relatives aux infractions, l'autorisation est nécessaire :
  - 2013-396 Défenseur des Droits : collecte d'éléments relatifs aux infractions;
  - 2013-141 CG Calvados : suivi de la fraude au RSA;
  - Les mutuelles ont l'obligation de transférer le casier judiciaire B2 des dirigeants à l'ACP
  - L'autorisation peut être refusée : 2013-377, Renault Trucks (détection de pédopornographie sur les postes de travail).

Échanges

frederic.thu@cabinet-cilex.com