Protection des données personnelles :
nouveaux risques et obligations tels qu'issus du Règlement général relatif à la protection des données (RGPD)

Nathalie Metallinos, avocate à la cour, Idea avocats

Chargée d'enseignement à l'université Paris Sud et au CNAM

Plan de la présentation

- Quelques rappels
- Contenu de la réforme
- Se préparer
- Questions/réponses

Rappels

Repères chronologiques

- **1978** : France : loi « informatique et libertés »
- 1980 : Lignes directrices de l'OCDE
- 1981 : Convention n°108 du conseil de l'Europe
- **1995** : Directive européenne 95/46 « protection des données personnelles »
- 1999 : Application de la directive 95/46 aux pays de l'AELE (Norvège, Islande et Lichtenstein)
- 2002 : Directive européenne 2002/58 « vie privée et communications électroniques »
- **2004** : Refonte de la loi Informatique et Libertés
- 2009 **:** Refonte du « paquet télécom »
- **2010 :** Reconnaissance droit à la protection des données personnelle comme un droit fondamental de l'UE **(art. 8** Charte européenne des droits fondamentaux)
- 2011 : Transposition dans les États membres de la réforme du paquet télécom
- 2016 : Adoption du nouveau Règlement européen relatif à la protection des données
- 2016 : Modification de la loi Informatique et libertés par la Loi pour une république numérique
- 2017 ? Adaptation de la directive vie privée et communications électroniques
- **2018** : entrée en vigueur du RGPD

Notions-clés (1)

La législation en matière de protection des données à caractère personnel s' applique aux **traitements** de **données à caractère personnel,** automatisés ou non => s' applique aux **traitements manuels** dès lors que les données sont appelées à figurer dans un **fichier**

⇒Il suffit que l'on puisse relier les données à la personne/que la personne soit affectée par les données pour que les données soient des données à caractère personnel

⇒Les données « anonymes » ne sont pas des données à caractère personnel (condition : impossibilité absolue de ré identifier la personne), sinon on parle de données « pseudonymes »

⇒ constituent des donnée à caractère personnel des données telles que le n° d'immatriculation d'un véhicule, l'adresse Mac du composant wifi d'un smartphone, l'adresse IP, un identifiant marketing implanté dans un cookie, une image, des données codées

Notions-clés (2)

Notions de Responsable de traitement et de sous-traitant

-**Le responsable de traitement**) est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (notion complexe)

- À distinguer de celle de sous-traitant = la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du responsable de traitement

Objectifs de la réforme

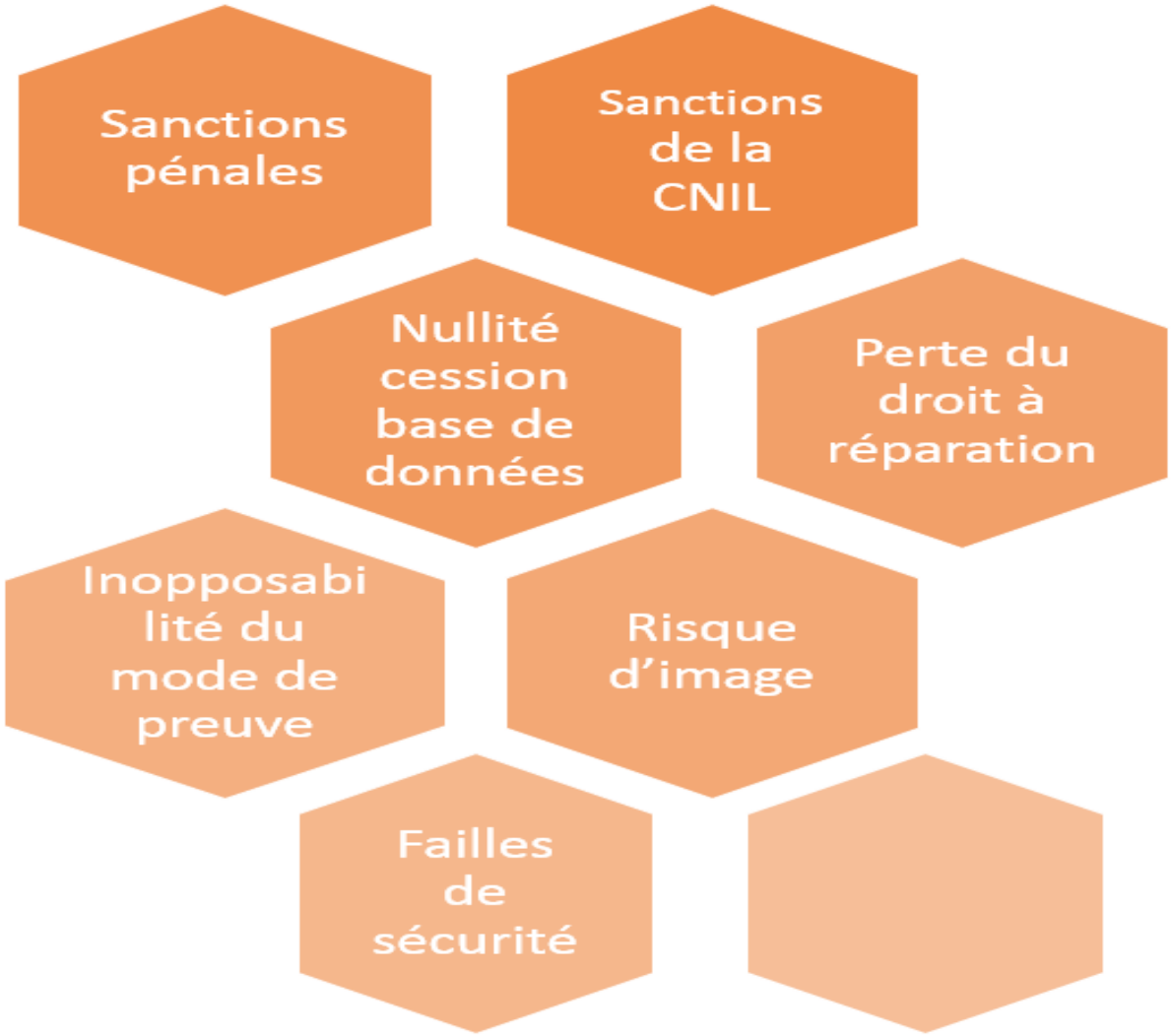
ADAPTATION DES PRINCIPES

- ✓ Faire face aux nouveaux défis technologiques et à l'importance croissante du volume des données personnelles traitées (**big data**)
- ✓ Prendre en compte la dissémination des données sur internet (**réseaux sociaux, informatique en nuage**)
- ✓ Tenir compte des modalités de collecte de moins en moins décelables (**Internet des objets**)

EFFECTIVITÉ DES RÈGLES

- ✓ Palier au manque d'harmonisation des règles, assurer la coordination rapide et efficace entre autorités nationales chargées de la protection des données.
- ✓ Rendre dissuasives les sanctions

Les Risques


Sanctions pénales
Sanctions de la CNIL
Nullité cession base de données
Perte du droit à réparation
Inopposabilité du mode de preuve
Risque d'image
Failles de sécurité

Le contenu de la réforme

Aperçu de la réforme en 8 points

1. Champ d'application étendu
2. Principes inchangés pour l'essentiel
3. Reconduction des restrictions (données particulières / transferts de données)
4. Le principe d'« accountability »
5. Le renforcement des droits des personnes
6. Les outils de la conformité
7. Le Nouveau régime de responsabilité
8. Application uniforme du Rgpd

1. Champ d'application étendu

Un champ d'application territorial étendu (art.3)

- **Principal critère reconduit :** l'établissement du responsable de traitement ou du sous-traitant
- **Nouvelles règles d'application extraterritoriale :** application aux responsable de traitement et sous-traitant non établis dans l'Union dès lors que les activités de traitement concernent des personnes physiques se trouvant sur le territoire de l'Union et
  - sont liées à l'offre de biens ou de services à ces personnes (y compris à titre gratuit), **ou**
  - au suivi du comportement de ces personnes (comportement qui a lieu au sein de l'Union).

Limites :

- **Sites Interne** : La simple accessibilité du site dans l'Union ne suffit pas à établir l'intention d'offrir des biens ou des services à des personnes situées sur le territoire de l'Union : application des critères du droit de la consommation (langue, monnaie, référents aux utilisateurs/clients situés dans l'Union)
- **Profilage**: le comportement suivi doit avoir lieu dans l'Union européenne

2. Des principes inchangés(1)

Conditions de licéité : Pour pouvoir être mis en œuvre le traitement de données à caractère personnel doit pouvoir être justifié par l'un des fondements suivants :

- le **consentement** de la personne concernée

- la nécessité **contractuelle**

- le respect d'une **obligation légale**

- la sauvegarde des **intérêts vitaux** de la personne concernée ou d'une autre personne physique

- l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique

- la poursuite des **intérêts légitimes** du responsable de traitement ou d'un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Important : Dans TOUS les cas le traitement doit être **compatible** avec les **finalités initiales** de la collecte.

2. Des principes inchangés(2)

Les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être (art.5):

- Obtenues et traitées de manière licite, loyale et transparente (**Licéité, loyauté et transparence**)
- Collectées pour des finalités déterminées, explicites et légitimes et ne sont pas utilisées ultérieurement de manière incompatible avec ces finalités (**Limitation des finalités**)
- Adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux finalités pour lesquelles elles sont traitées (**Minimisation des données**)
- Exactes et si nécessaire tenues à jour (**Exactitude**)
- Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (**Limitation de la conservation**) Exceptions : archives publiques, recherche scientifique & historique
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (**intégrité et confidentialité**)

3. Reconduction des restrictions : les catégories particulières de données

Données « sensibles » (art.9)

- Qui font apparaître, directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes,
- traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique,
- Ou qui sont relatives à la santé ou la vie sexuelle

Interdiction pouvant être levée par le jeu d'exceptions prévues dans le Rgdp

Infractions, condamnations et mesures de sûreté (art.10)

- Ne peut être effectué que sous le contrôle de l'autorité publique, ou
- Si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre
- Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Données relatives aux mineurs (art.8)

- Offres des services de la société de l'information : Exigence de consentement parental pour les enfants de moins de 16 ans

3. Reconduction des restrictions : les transferts de données hors UE

Principes (art.44 à 50)

Les transferts ne doivent pas compromettre le niveau de protection garanti par le Rgpd (// CJUE Schrems)

Renforcement des conditions de l'adéquation

Nouveau rôle reconnu aux règles internes d'entreprise (BCR), aux codes de conduite et à la certification

Reconduction du jeu des exceptions

Dispositions applicables également aux transferts ultérieurs

En pratique

Transferts **libres** vers les pays/secteurs d'activités « adéquats »

Transferts **libres** moyennant la mise en œuvre de garanties adéquates (à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives) :

- ✓Accords entre autorités & organismes publics
- ✓Clauses contractuelles types
- ✓Règles internes d'entreprise
- ✓Code de conduite
- ✓Certification

Dans les autres cas: **Autorisation** de l'autorité de protection des données

sauf si exceptions applicables

4. Nouveau principe d' « accountability »

Changement de philosophie : vers un régime d'autorégulation

- Obligation de **démontrer** la conformité aux principes **(art.5-2) et notamment** la mise en œuvre des mesures techniques **et organisationnelles**
- **Art.24 : Approche par les risques «** Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. »

Conséquence :

- Adoption de politiques internes et codes de conduite (notamment pour les transferts)
- Mise en place de systèmes de contrôle(audit des traitements, certification)
- Réalisation d'études d'impact sur la vie privée,

5. Les outils de la conformité

Le DPO (section IV)

Le contrôle renforcé du recours à la sous-traitance (art.28)

La tenue du registre des activités de traitement (art.30)

L'analyse d'impact (EIVP) (art.35)

La consultation préalable de l'autorité de contrôle (art.36)

Les codes de conduite (art.40) et certifications (art.42)

La mise en œuvre du privacy by design/by default (art.33)

Les BCR (art.47)

6. Renforcement des droits des personnes

- Droit à l'information renforcé (art.13-15)
  - Information sur le fondement du traitement, sur la durée de conservation (//LRN), le droit de retrait du consentement donné, accès à la logique qui sous-tend les mesures de profilage, sur les traitements ultérieurs…
- Droits de rectification, droit à l'effacement et à la limitation du traitement (art.17&18)
- Droit à la portabilité des données si traitement repose sur le consentement ou est effectué à l'ide de procédés automatisés (art.20)
- Renforcement de la charge de preuve pour l'exercice du droit d'opposition (art.21)
- Droit d'opposition au profilage à des fins de prospection (art.221-2), ainsi qu'aux prises de décisions basées sur le profilage (art.22)
- Droit à réclamation auprès de l'autorité de contrôle, droit à un recours juridictionnel, droit à réparation + action de groupe (organismes/associations œuvrant à la protection des personnes)
- Condition de consentement (non valide si « déséquilibre significatif »)
- Traitement des données relatives aux mineurs

7. Nouveau régime de responsabilité

Droit à réparation des personnes (actions de groupe)

Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du règlement.

Fin du régime d'immunité du sous-traitant :

Obligations et responsabilité propre

=> responsable du dommage causé par le traitement

1) s'il n'a pas respecté ses obligations spécifiques ou

2) s'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Solidarité vis à vis de personnes concernées

Des **sanctions alourdies** : jusqu'à 20millions d'euros (ou 4% CA mondial)

8. Application uniforme du Rgpd

Instauration d'un principe de guichet unique

Assistance mutuelle entre autorité de protection des données (échanges d'informations, contrôles conjoints)

Mécanisme de contrôle de cohérence

Création du Comité européen de la protection des données (CEPD)

Se prépare à l'entrée en application du Rgpd

LES ACTIONS À METTRE EN ŒUVRE

Réaliser un État des lieux (1)

État des lieux = première étape pour assoir une démarche de conformité

Objectifs :

- recenser les traitements
- disposer d'une appréciation générale sur la conformité des traitements mis en œuvre, afin de mettre en place un plan d'action
- permettre l'encadrement et la diffusion de bonnes pratiques, ainsi que de mesure du risque opérationnel résultant de ces traitements.

Gouvernance et procédures (2)

Adoption de politiques / gouvernance destinées à assurer l'application du Règlement général relatif à la protection des données à caractère personnel

- Organisation et responsabilités (RACI)
- Politique de durée de conservation et archivage
- Analyse des risques
- Procédure de réalisation des EIVP
- Respect des droits des personnes
- Traitement des réclamations des personnes
- Coopération avec l'autorité de contrôle

Déploiement opérationnel(3)

- Formation et la sensibilisation des personnels à la règlementation I&L
- Réécriture des mentions d'information
- Revue des modèles de contrats de sous-traitance (pour inclure notamment la liste de obligations auxquelles est tenu le responsable de traitement)
- Établissement de conventions intragroupe pour répartir les responsabilités des traitements
- Revue des contrats prestataires (renégociation, répartition des responsabilités en cas de responsabilité conjointe) et audits
- Réalisation d'études d'impacts sur les nouveaux traitements

Des questions ?

Merci de votre attention

Nathalie.metallinos@idea-avocats.com