La RGPD et la protection des données dans le monde

Clément Levallois

2018-06-20

Table of Contents

last modified: 2019-01-02

1. Evolution de la réglementation de la protection des données dans l'UE

a. La directive sur la protection des données de l'UE en 1995

La présente directive découle des lignes directrices antérieures adoptées par l'OCDE dès 1980 sur la protection de la vie privée et les flux transfrontières de données personnelles.

Ces lignes directrices ont été adoptées par les membres de l'OCDE mais n'étaient pas contraignantes: par exemple, les États-Unis n'ont pas traduit les lignes directrices de l'OCDE sur la protection de la vie privée dans leur législation. En revanche, ces lignes directrices ont été transformées en directive par l'UE en 1995.

- tout le texte de la directive européenne sur la protection des données
- Présentation de la directive de l'UE sur la protection des données

Cette directive garantit et facilite la libre circulation des données à caractère personnel entre les États membres de l'UE, en fournissant un cadre valable pour tous les États membres pour la protection des données à caractère personnel des citoyens de l'UE. **Cela répond à la volonté de créer un marché commun, qui doit évoluer dans un cadre réglementaire uniforme**.

Comment est traitée la question des données de l'UE détenues par des sociétés non européennes? Par exemple, quel est le niveau de protection des données personnelles d'un individu français appartenant à une entreprise américaine sur un serveur situé aux États-Unis?

→ Selon la directive de 1995, la règle était simple: **il est interdit d'exporter des données personnelles vers un pays hors UE avec un niveau plus faible de protection des données personnelles.**

b. Le cas des données sur les citoyens de l'UE hébergées par des entreprises américaines

L'affaire est importante car les principaux fournisseurs de services impliquant des données

personnelles (google search, gmail, gmaps, facebook, etc.) sont hébergés aux États-Unis.

La question est: quel est le niveau de protection des données dans ce cas? Niveau de protection américain ou UE?

Il ne devrait pas être possible d'héberger des données personnelles des citoyens de l'UE aux États-Unis parce que les États-Unis ont des réglementations beaucoup moins strictes en la matière. En effet, aux États-Unis:

- Il existe un cadre réglementaire sur la protection des données pour les données collectées ou détenues par le gouvernement fédéral.
- Mais il n'existe pas de cadre général sur la protection des données en dehors du gouvernement fédéral (niveau des États).

Pour remédier à cette situation, les principes du Safe Harbor sont un accord international entre les États-Unis et l'UE qui a été mis en place en 2000.

Les principes du Safe Harbor sont une série de règlements que les entreprises américaines peuvent accepter de suivre si elles veulent héberger des données personnelles l'UE sur le sol américain. Ces règles fournissent un niveau de protection des données équivalent à celui garanti par la directive sur la protection des données de 1995 dans l'UE.

En Octobre 2015, Maximillian Schrems (un étudiant en droit en Autriche) a lancé une action en justice contre Facebook pour défaut de protection de ses données personnelles contre l'espionnage de la NSA aux Etats-Unis.

La défense de Facebook était de faire valoir qu'elle était conforme à la Safe Harbor Act. La plainte a été portée devant la Cour européenne de justice, qui a fini par déclarer **invalide le Safe Harbor Act** parce que:

```
"Une législation permettant aux pouvoirs publics d'accéder de manière généralisée au
contenu des communications électroniques doit être considérée comme compromettant
l'essence même du droit fondamental au respect de la vie privée".
```

Les mois suivants ont été marqués par une incertitude juridique car les données de l'UE hébergées sur des serveurs américains ne l'étaient plus dans des conditions légales - le Safe Harbor Act avait cessé d'exister.

Le 2 février 2016, l'UE et les États-Unis ont créé un nouvel accord juridique connu sous le nom de EU-US Privacy Shield, qui est le successeur du Safe Harbor Act. Le Privacy Shield diffère du Safe Harbor Act dans ce qui suit:

1. Des obligations plus fortes pour les entreprises aux États-Unis de protéger les données personnelles des Européens et de renforcer le contrôle et l'application par le Département du Commerce des États-Unis et la Federal Trade Commission.
2. L'accès aux données personnelles transférées en vertu du nouvel arrangement par les autorités publiques aux États-Unis devait être soumis à des conditions, des limites et une surveillance claires, empêchant l'accès généralisé des organismes de surveillance de l'État.

3. Protection effective des droits des citoyens de l'UE avec plusieurs possibilités de recours.
4. Un mécanisme d'examen conjoint annuel entre l'UE et les États-Unis.

c. RGPD, un nouveau cadre légal

Le traitement des données des citoyens de l'UE en dehors de l'UE est d'une grande complexité juridique, comme en témoigne la fragilité des accords juridiques entre l'UE et les États-Unis. L'UE devrait-elle créer des accords juridiques spéciaux avec tous les pays souhaitant que leurs entreprises puissent héberger des données personnelles de l'UE? Cela ressemble à un cauchemar bureaucratique (ou au rêve d'un avocat). Au lieu de cela, l'UE a conçu **un nouveau principe juridique** s'appliquant à tous les pays détenant des données personnelles de l'UE, sans avoir besoin d'accords bilatéraux. **Ceci est le RGPD**.

Le **RGPD: Règlement général sur la protection des données** est un cadre juridique entré en vigueur en 2018 qui remplace la directive de 1995 par une nouvelle règle simple: les données des citoyens de l'UE doivent être traitées conformément aux règles établies par l'UE

Avant d'examiner le RGPD plus en détail, nous définissons les termes juridiques qui y sont utilisés:

2. Définitions clés

Source pour ces définitions de clé: un livre blanc synthétique sur le RGPD par Dataiku et le glossaire de la CNIL.

a. Données personnelles

Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale…).

b. Données sensibles

Les données sensibles constituent une catégorie particulière de données personnelles (notamment données personnelles révélant l'origine raciale ou ethnique, opinions politiques, croyances religieuses ou philosophiques, appartenance à un syndicat, données sur la santé ou la vie sexuelle) à laquelle des protections supplémentaires s'appliquent.

c. Personne concernée

Une personne concernée est un être humain sur lequel des données personnelles sont collectées.

d. Responsable de traitement ("Data controller" en anglais)

Un responsable de traitement est une entité qui détermine les objectifs, les conditions et les

moyens du traitement des données personnelles. Lorsque l'organisation est suffisamment grande, une position dédiée de "Responsable de traitement" peut être créée, sinon c'est le responsable légal de l'organisation.

Ex: en France, le responsable de traitement est chargé de déclarer les données personnelles traitées à la CNIL.

e. Sous-traitant ("Data processor" en anglais)

Un sous-traitant est une entité qui traite des données personnelles pour le compte du responsable de traitement (par exemple, fournisseurs d'hébergement cloud et de centre de données).

Jusqu'en 2017, il a été considéré que le sous-traitant "exécute" simplement la mission donnée par le responsable de traitement:

- le sous-traitant est chargé des mesures de sécurité appropriées pour assurer la protection des données contre la violation, la perte ...
- mais le sous-traitant n'est pas responsable des procédures de collecte inappropriées des données personnelles établies par le responsable du traitement.

À partir de 2018 avec le RGPD, **le sous-traitant est co-responsable avec le responsable de traitement en cas de violation de données compromettant les données personnelles des personnes concernées**.

4. Quatre principes clés pour le traitement légitime des données personnelles

a. Consentement préalable

Le consentement préalable est requis avant de recueillir des données personnelles en vue de leur traitement:

- La politique de collecte de données doit être clairement mise à la disposition des utilisateurs
- L'exclusion doit être possible
- Le consentement doit être présenté clairement

b. Adéquation / objectif légitime

Les données collectées doivent être exactement nécessaires pour exécuter le service, pas plus.

Time out: les informations doivent être supprimées lorsque le service s'arrête. En France, il y a une limite de 13 mois après laquelle le consentement doit être renouvelé.

c. Portabilité

→ L'information doit être disponible sur demande

En 2011, Max Schrems a demandé toutes ses données Facebook. Il en a reçu 1200 pages.

Grâce à ses efforts, maintenant la plupart des médias sociaux offrent un téléchargement en un clic de vos données personnelles.

La portabilité couvre également le «droit à l'oubli», détaillé sur dans cette article.

d. sécurité

Toutes les précautions raisonnables doivent être prises contre les violations de données. Les précautions prises devraient être proportionnées aux dommages qui résulteraient d'une violation de la sécurité.

Notions de base: définir et gérer les droits d'accès à chaque aspect pertinent des données. Les utilisateurs doivent être informés des violations de sécurité susceptibles d'affecter leurs données

5. En 2018: le RGPD et ce qu'il change

RGPD signifie "Règlement Général sur la Protection des Données". Il a été adopté par l'UE le 14 avril 2016 et est appliqué depuis le **25 mai 2018**.

Ses principales nouveautés, par rapport à la directive européenne sur la protection des données, sont:

a. Application

Le RGPD s'applique à toute entreprise (**quel que soit son emplacement**, sa taille et son secteur) traitant les données personnelles des personnes résidant dans l'UE. Par exemple, une entreprise qui traite les données personnelles aux États-Unis de citoyens de l'UE est tenue de se conformer au RGPD.

b. Responsabilité

Sous le RGPD, le responsable de traitement et le sous-traitant doivent se conformer à la législation. En vertu de la directive précédente sur la protection des données, seuls les responsables du traitement des données étaient tenus responsables de la conformité à la protection des données, et non des processeurs de données.

c. Pénalités

Avec une amende pouvant aller jusqu'à 4% du chiffre d'affaires global annuel ou 20 millions d'euros (selon le montant le plus élevé), les pénalités pour non-conformité sont élevées.

d. Consentement

En vertu du RGPD, les entreprises ne pourront plus utiliser des termes longs et illisibles remplis de jargon juridique; consentement pour la collecte et l'utilisation des données personnelles doit être en langage clair et en détail le but du traitement des données.

e. Les violations de données

Réglementation accrue entourant la divulgation de **violations de données** . Plus précisément, des rapports beaucoup plus rapides sont requis (dans les 72 heures).

f. Droits des sujets de données

Les personnes concernées dans l'UE ont élargi leurs droits en matière de protection des données, notamment:

- le droit à l'oubli (effacement de leurs données),
- le droit d'accès (obtenir des informations sur exactement quelles données sont traitées où et dans quel but),
- et le droit à la portabilité des données (recevoir une copie des données personnelles les concernant).

Les citoyens ont maintenant également le droit de questionner et remettre en cause les décisions qui les affectent sur une base purement algorithmique.

g. Confidentialité "by design"

Confidentialité by design est une obligation légale de considérer la confidentialité des données dès le début de tous les projets et initiatives, et non après coup.

h. Nomination d'un délégué à la protection des données (DPD)

Les Contrôleurs et processeurs dont le cœur de métier est le suivi régulier et systématique des données personnelles à grande échelle ou qui traitent de catégories particulières de données, devront désigner un délégués à la protection des données. Le DPD peut être nommé en interne, embauché ou sous contrat, mais (parmi d'autres exigences spécifiques) il doit être un expert en droit et en pratiques de protection des données.

6. Protection des données: un aperçu rapide en dehors de l'UE

a. ETATS-UNIS

- Cadre sur la protection des données pour les données collectées / détenues par le gouvernement fédéral
- Mais pas de cadre général sur la protection des données en dehors du gouvernement fédéral

b. Inde

IT Act de 2000 + Règlement IT 2011

- Met l'accent sur les informations personnelles **sensibles**: mots de passe, informations financières, état de santé, orientation sexuelle, informations biométriques.
- Pas besoin de déclarer les activités de traitement de données à une autorité

c. Chine

En Chine, la protection des données n'est pas promulguée dans une seule loi, à l'exception de lois de portée plus large: le Comité permanent du Congrès national du peuple a promulgué une Décision concernant le renforcement de la protection de l'information sur les réseaux. La Chine a plutôt des textes législatifs sectoriels, tels que le règlement sur la protection des renseignements personnels des utilisateurs de services de télécommunication et d'Internet (MIIT Regulation).

L'Etat chinois développe des initiatives telles que le Système de Crédit social qui reposent sur un système de surveillance de masse, en opposition à la libre maîtrise pour un individu de ses données personnelles.

d. Législation pour la protection des données personnelles dans d'autres pays

Pour avoir une vue synthétique des lois sur la protection des données dans d'autres pays, visitez ce site Web par Thomson Reuters.

Pour aller plus loin

Retrouvez le site complet : ici.

Clement Levallois

Découvrez mes autres cours et projets : https://www.clementlevallois.net

Ou contactez-moi via Twitter: @seinecle