

ISAE-SUPAERO



LE DROIT DES DONNÉES PERSONNELLES

Mélanie Gornet, Télécom Paris
melanie.gornet@telecom-paris.fr

Importance de la donnée

**Les données personnelles :
le pétrole du 21ème siècle**



Refuser et s'abonner pour 1€ →

Soutenez [redacted] ! Dites oui

Nous et nos partenaires utilisons des technologies comme les cookies pour stocker et/ou accéder à des informations personnelles non sensibles stockées sur votre terminal (identifiants uniques, ...), que nous traitons afin de réaliser des statistiques d'usage du site, personnaliser les publicités et le contenu et en mesurer les performances, produire des données d'audience, développer et améliorer les produits. Ces technologies peuvent utiliser des données de géolocalisation précises ou analyser activement les caractéristiques du terminal pour l'identification.

Cliquez sur le bouton « Oui, j'accepte » pour consentir à ces utilisations sur ce site, sur « Paramétrages » pour paramétrer vos choix et/ou vous opposer lorsque l'intérêt légitime est utilisé ou sur « Refuser et s'abonner pour 1€ ».

Vous pouvez à tout moment revenir sur vos choix en utilisant le lien « Paramétrages » disponible dans notre page de gestion des cookies.

Oui, j'accepte

Paramétrages

Enjeux démocratiques

Politique / Société

Cambridge Analytica, l'incarnation de la triche électorale rendue possible par Facebook

April Glaser — Traduit par Jean-Clément Nau — 21 mars 2018 à 8h58 — mis à jour le 21 mars 2018 à 9h14

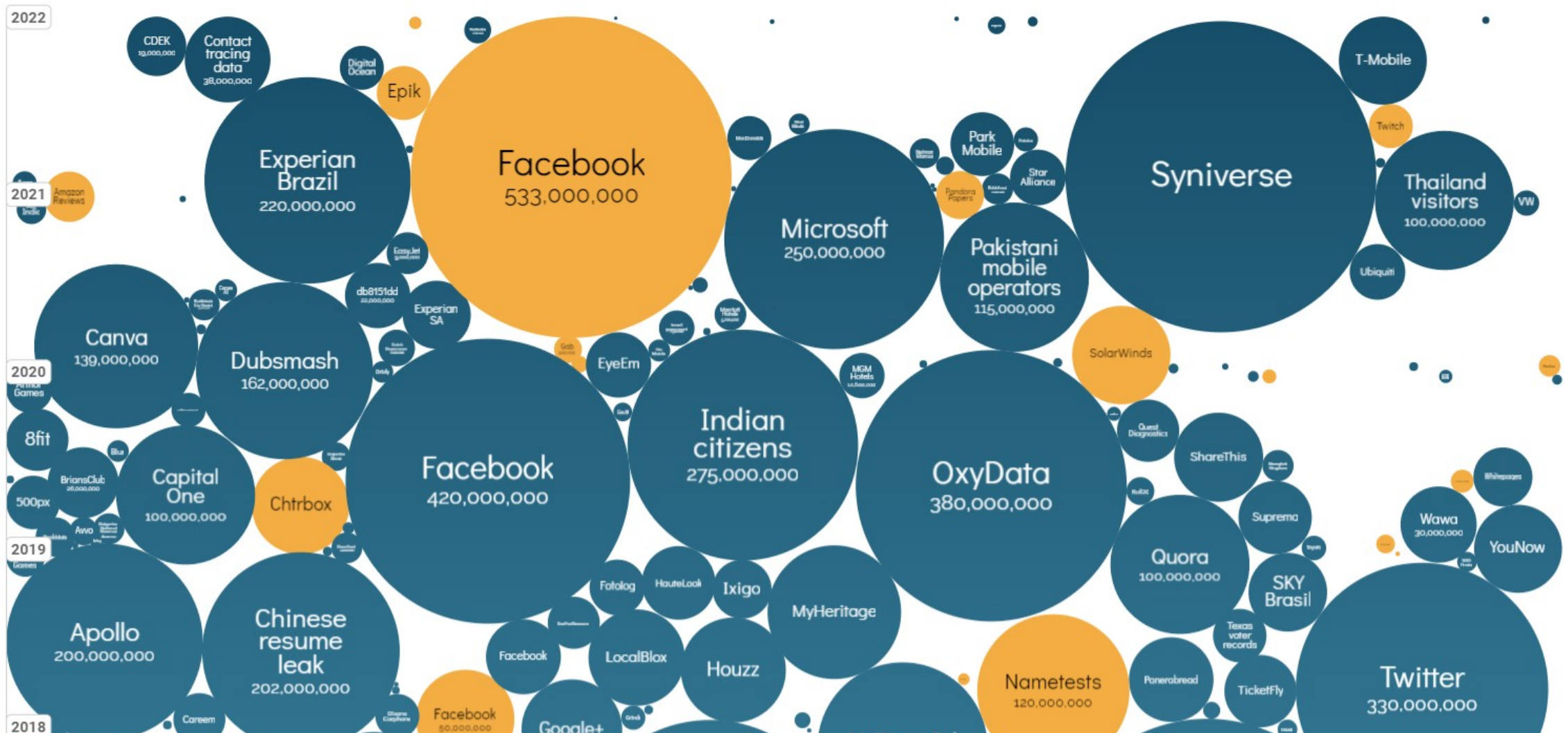
Pendant la campagne électorale de 2016, la campagne de Donald Trump aurait fait main basse sur les données de cinquante millions d'utilisateurs.

Scandale Cambridge Analytica - Facebook



« Derrière nos écrans de fumée », Netflix ([Bande annonce](#))

Enjeux de sécurité des données



World's Biggest Data Breaches & Hacks ([lien](#))

Le droit à la vie privée

Un droit fondamental, protégé par les textes internationaux, européens et nationaux :

- Article 12 de la Déclaration Universelle des Droits de l'Homme des Nations Unies ([lien](#))
- Article 8 de la Convention Européenne des Droits de l'Homme ([lien](#))
- Article 9 du Code Civil ([lien](#))

✉ Englobe le droit à la protection des données à caractère personnel, protégé par :

- Article 8 de la Charte des Droits Fondamentaux de l'Union Européenne ([lien](#))



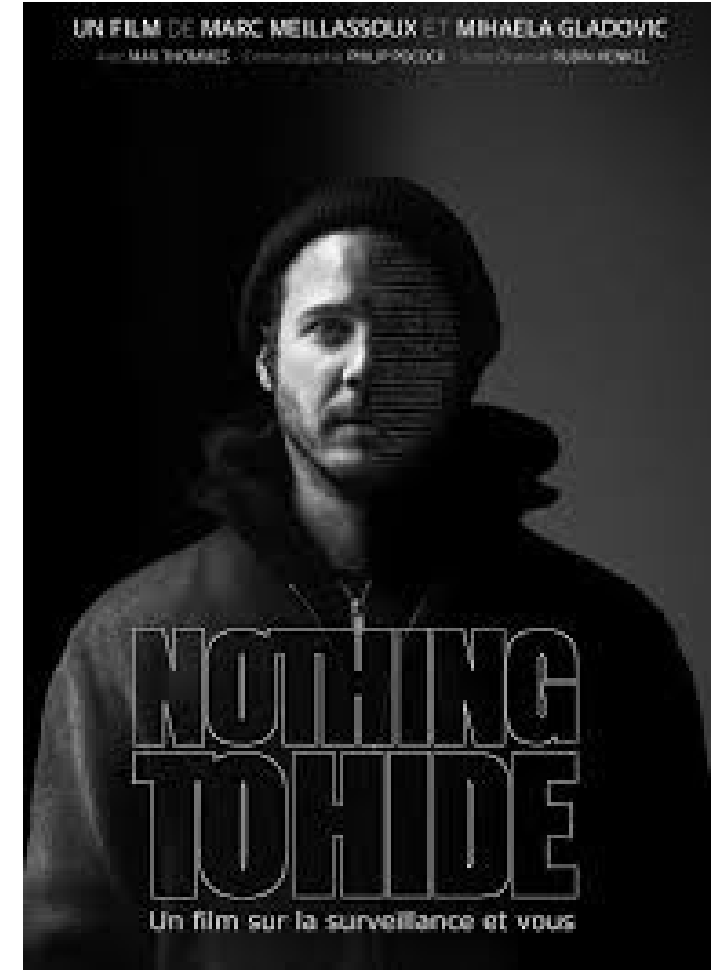
Le droit à la vie privée



Capitalisme de surveillance,
Shoshanna Zuboff ([vidéo](#))



*« Arguing that you don't care
about the right to privacy
because you have nothing to
hide is no different than saying
you don't care about free
speech because you have
nothing to say »*
- Edward Snowden



Nothing to hide
([bande annonce](#), [film](#))

Historique international et européen 1/2

- 1980 : OCDE Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ([lien](#))

7 principes :

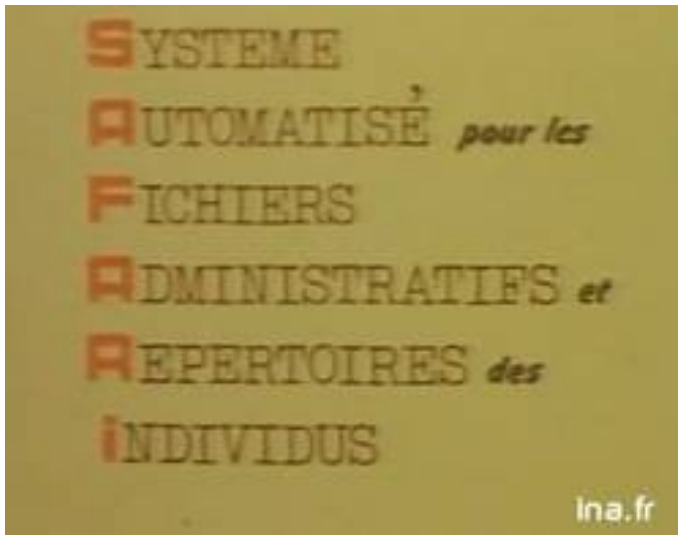
- limitation en matière de collecte
 - qualité des données
 - limitation de l'utilisation
 - garanties de sécurité
 - participation individuelle
 - responsabilité
- 1981 : Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ([lien](#))

Historique international et européen 2/2

- 1995 : Directive 95/46/CE sur la protection des données personnelles ([lien](#))
- 2000 : Charte des Droits Fondamentaux de l'Union Européenne ([lien](#))
- 2012 : Groupe de travail « article 29 », Avis 01/2012 sur les propositions de réforme de la protection des données ([lien](#))
- 2016 : Règlement UE 2016/679 sur la protection des données (RGPD) ([lien](#))
- 2018 : entrée en vigueur du RGPD

Historique français de la réglementation 1/2

Le projet SAFARI



... LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la Justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur

puissant destiné à rassembler la masse énorme des renseignements graphiés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à décrire chaque Français par un « identifiant », qui ne définit pas que lui, maintenant terminé, est l'objet de convois incessants; le ministère de l'intérieur y souhaite

jouer le premier rôle. En effet, une telle banque de données, sous-jacent opérationnel de toute autre collecte de renseignements, donnera à qui la possèdera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique.

Son importance exigerait qu'il en soit, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la Justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

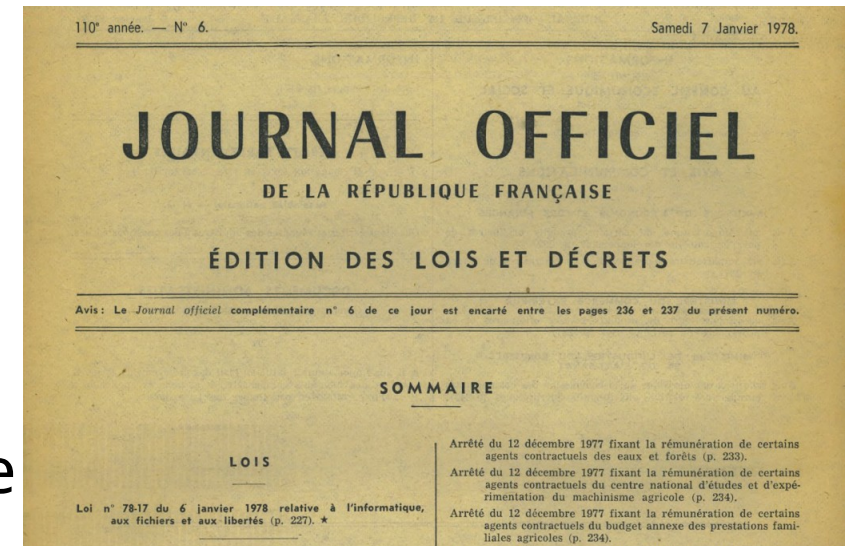
« Safari » ou la chasse aux Français

- 1970 : le député Michel Poniatowski propose à l'Assemblée nationale la création d'un comité de surveillance et d'un tribunal de l'informatique, la suggestion est rejetée
- 1971 : Projet SAFARI d'interconnexion de fichiers nominatifs
 - Centralisation des données
 - Utilisation du NIR pour vérifier l'identité des personnes
 - Faciliter les études statistiques de la population
- 1974 : Révélation du projet par le journal *Le Monde*

Historique français de la réglementation 2/2

La Loi Informatique et Libertés

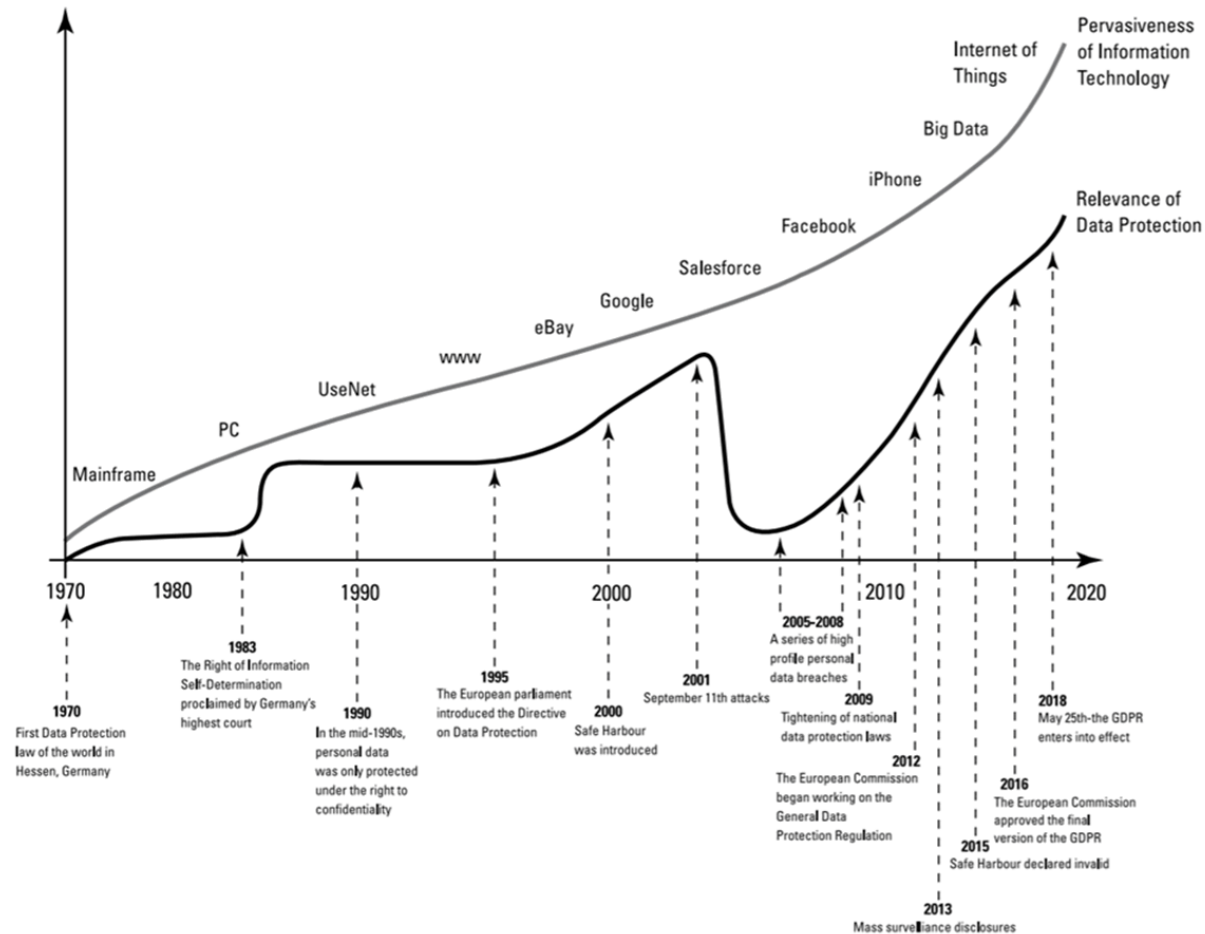
- 1978 : Première version de la LIL après le scandale du projet SAFARI
 - Création d'une autorité nationale de protection des données personnelles
- 2004 : réforme de la LIL pour la transposition libre de la Directive de 95
 - « informations nominatives » devient « données à caractère personnel »
 - accroît les pouvoirs de la CNIL pour les contrôles et les sanctions
- Déc 2018 : mise en cohérence de la LIL avec le RGPD ([lien](#))



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Evolution de la protection des données personnelles

The Rise of Information Technology in the World Economy






Le Règlement Général à la Protection des Données personnelles (RGPD)

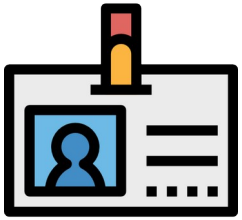


- Voté en 2016 et entré en vigueur le 25 Mai 2018, remplace la directive européenne de 1995 ([lien](#))
- Intégré à un paquet européen
- Logique de mise en conformité
- 2 objectifs :
 - Protéger les données personnelles
 - Permettre la libre circulation des données au sein de l'Union
- Application large
- Sanctions très importantes en cas de violation

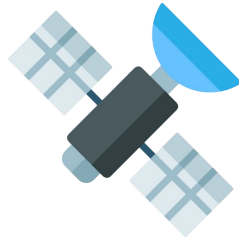
I. Champ d'application

1. Champ d'application matériel  « quoi »
2. Champ d'application territorial  « où »
3. Champ d'application personnel  « qui »

Qu'est-ce qu'une donnée personnelle ?



Nom / Prénom



Photos
satellites



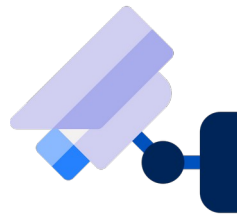
Numéro de
téléphone
d'une
entreprise



Adresse email
professionnell
e



Régime
alimentaire d'un
client



Enregistrement
vidéosurveillanc
e

Une adresse IPv4 (notation décimale à point)

172 . 16 . 254 . 1

Adresse IP

La notion de donnée à caractère personnel

Définition : « *Toute information se rapportant à une personne physique identifiée ou identifiable* »

Art. 4.1 RGPD

Identification directe : nom/ prénom ; numéro de sécurité sociale ;

empreinte digitale
Identification indirecte : plaque d'immatriculation, numéro de téléphone, adresse IP ...



La personne identifiée ou identifiable est appelée la « personne concernée »



Données personnelles « sensibles »

Données révélant de :

- L'origine raciale ou ethnique ;
- L'opinion politique ;
- Les convictions religieuses ou philosophiques ;
- L'appartenance syndicale ;
- Les données génétiques ou biométriques ;
- Les données de santé ;
- La vie sexuelle ou orientation sexuelle ;

✉ Ne peuvent pas faire l'objet d'un traitement (sauf exception)

Art. 9 RGPD

La notion de traitement de données

Définition : « 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 à caractère personnel »

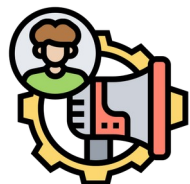
Art. 4.2 RGPD

Exemples : 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



- Toute action en rapport avec des données personnelles est un traitement !
- Toutes les entités réalisent des traitements !

Les personnes redevables



Responsable(s)
de traitement

- **Choisit les finalités et les modalités** du traitement
Art. 4.7 RGPD
- **Maîtrise intellectuelle** du traitement
- **Responsabilité** civile et pénale en cas de manquement



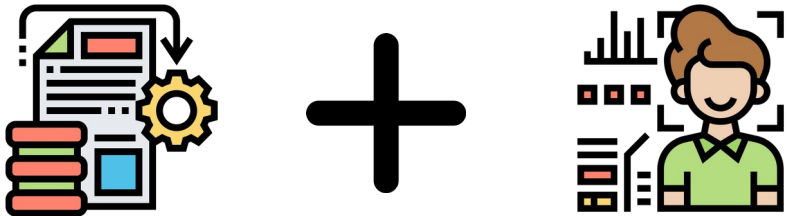
Sous-traitant

- Traite les données **pour le compte du responsable** de traitement Art. 4.8 RGPD
- **Maîtrise technique** du traitement
- Doit **respecter les directives** du responsable de traitement ET les règles sur les données personnelles



Responsabilité solidaire entre le responsable de traitement et le sous-traitant pour la personne concernée

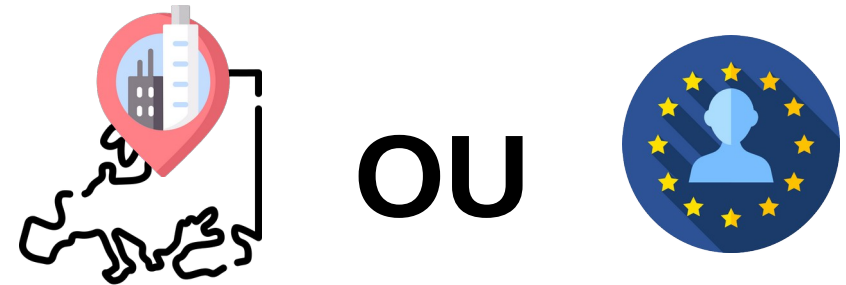
Champ d'application matériel



Présence d'un traitement de données à caractère personnel

Art. 2 RGPD

Champ d'application territorial



Le responsable de traitement ou le sous-traitant se situe sur le territoire de l'EEE

OU

Les personnes concernées se trouvent sur le territoire de

l'EEE

Art. 3 RGPD

II. Régime « comment »

1. Les obligations
2. Les droits

Licéité du traitement

Le RGPD pose une liste de 6 justifications possibles pour rendre un traitement licite :

- 1 Le **consentement** de la personne concernée
- 2 **Exécution d'un contrat** avec le responsable de traitement
- 3 Respect d'une **obligation légale**
- 4 Sauvegarde **des intérêts vitaux** d'une personne physique
- 5 Réalisation d'une **mission d'intérêt public**
- 6 Nécessaires à la réalisation des **intérêts légitimes**

Art. 6.1 RGPD



Finalités du traitement

1

Les finalités doivent être **déterminées, explicites et légitimes.**

2

Les données doivent être traitées exclusivement pour atteindre la/les finalité(s) choisies !

Art. 5.1 RGPD

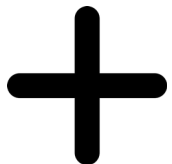
Conséquences : Toutes vos actions sur les données doivent être proportionnelles avec les finalités ✉ principe de **minimalisation** des données



- Pas de recours à des moyens disproportionnés

- On ne récolte pas de données si elles ne sont pas nécessaires

- Pas de réutilisation des données personnelles pour traitement ultérieur (sauf exceptions)

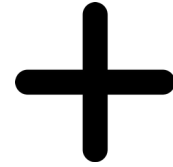


Principe de **loyauté** et de **transparence** : la personne concernée doit savoir que ses données font l'objet d'un traitement et doit connaître la finalité du traitement.

Exigences sur les données



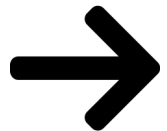
**Données
exactes**



**Données tenues à
jour**



- Possibilité de corriger ses données
- Effectuer la modification dans les différentes bases contenant la donnée en question
- Répercuter ce changement sur les décisions prises sur le fondement de cette donnée
- Vérifier régulièrement l'exactitude des données en cas de changement de contexte



Supprimer rapidement des données erronées ou obsolètes !



La durée de conservation

1

Définir la durée

Conservation
proportionnelle à la finalité
du traitement

Exemples de durée maximum:

- Pour les cookies = **13 mois**
- Pour les vidéos de surveillance = **1 mois**

2

Après la fin du délai

- Suppression des données, ou
- Conservation dans un but de recherche ou de statistiques, ou
- Anonymisation des données.

Transfert de données hors de l'UE 1/3

RAPPEL Si les données proviennent d'européen ou sont traitées en UE, la réglementation (RGPD) s'applique à ces données



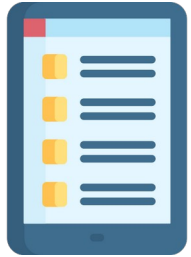
Toutes ces données doivent bénéficier d'un niveau de protection uniforme !



Protection équivalente obligatoire pour tous les acteurs impliqués dans le traitement de données, même s'ils sont situés hors de l'UE

Transfert de données hors de l'UE 2/3

Conséquences pratiques



- Lister les individus ayant un droit d'accès aux données.
- Conserver pour chaque destinataire / utilisateur de données le type de donnée auxquels il a accès / qu'il a reçu.



- Identifier les pays où les données sont situées et transférées.
Identifier les pays où résident ceux ayant accès aux données.



- Communiquer ces informations au service juridique et collaborer avec lui si besoin.

Si les données sont transmises à des personnes non conformes à la réglementation, votre entreprise est sanctionnable !

Transfert de données hors de l'UE 3/3

La notion de décision d'adéquation

Une décision de la Commission européenne établissant qu'un pays tiers, par l'intermédiaire de sa législation interne ou de ses engagements internationaux, offre un niveau de protection des données à caractère personnel comparable appliqué dans l'Union européenne.

L'exemple des Etats-Unis



→ **Annulation
par la CJUE
(2015)**



→ **Annulation
par la CJUE
(2020)**

Sécurité et Violation de données

DÉFINITION : destruction, perte, altération, divulgation non autorisée ou accès non autorisé, de manière accidentelle ou intentionnelle, de données à caractère personnel.

1 Avant la faille de sécurité

- Mise en place des mesures organisationnelles et techniques proportionnées :



- Chiffrement
- Mot de passe sécurisé
- Eviter le BYOD
- Back up régulier ...

✉ principe de **sécurité**

2 Après la faille de sécurité

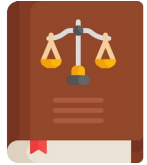
- Notification à l'autorité de contrôle dans les plus brefs délais
- Expliquer le contexte et les conséquences potentielles de la faille :



- Décrire les données concernées
- Lister les personnes concernées
- Et répondre à tout autre question interne

✉ principe d'**information**

Droit à l'information



Dans les textes :

Informations à communiquer à la personne concernée :

- Identité du responsable de traitement ;
- Finalités du traitement ;
- Base légale ;
- Destinataires de vos données ;
- Durée de conservation ;
- Droits de la personne concernée ;
- ...

Art. 12 RGPD



Dans la pratique :

ARTICLE 1 : Objet

Les présentes « conditions générales d'utilisation » ont pour objet l'encadrement juridique des modalités de mise à disposition des services du site [Nom du site] et leur utilisation par « l'Utilisateur ».

Les conditions générales d'utilisation doivent être acceptées par tout Utilisateur souhaitant accéder au site. Elles constituent le contrat entre le site et l'Utilisateur. L'accès au site par l'Utilisateur signifie son acceptation des présentes conditions générales d'utilisation.

Éventuellement :

- En cas de non-acceptation des conditions générales d'utilisation stipulées dans le présent contrat, l'Utilisateur se doit de renoncer à l'accès des services proposés par le site.
- [Nom du site] se réserve le droit de modifier unilatéralement et à tout moment le contenu des présentes conditions générales d'utilisation.

ARTICLE 2 : Mentions légales

L'édition du site [Nom du site] est assurée par la Société [Nom de la société] [SAS / SA / SARL, etc.] au capital de [montant en euros] € dont le siège social est situé au [adresse du siège social].

[Le Directeur / La Directrice] de la publication est [Madame / Monsieur] [Nom & Prénom].

Éventuellement :

- [Nom de la société] est une société du groupe [Nom de la société] [SAS / SA / SARL, etc.] au capital de [montant en euros] € dont le siège social est situé au [adresse du siège social].

L'hébergeur du site [Nom du site] est la Société [Nom de la société] [SAS / SA / SARL, etc.] au capital de [montant en euros] € dont le siège social est situé au [adresse du siège social].

ARTICLE 3 : Définitions



J'ai lu et j'accepte les conditions

Droit d'accès aux données personnelles



Dans les textes :

Informations à communiquer sur demande :

- Les informations vues précédemment
- Les données que possède le responsable de traitement ;
- La « logique sous-jacente » de l'algorithme utilisé le cas échéant ;
-



Dans la pratique :





Google Dashboards





Paramètres > Vos données twitter

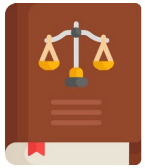


Raccourcis de confidentialité

	Droit à la rectification	Droit à la limitation	Droit d'opposition
Définition et Objectif 	<ul style="list-style-type: none"> • Corriger les données inexactes • Compléter les données existantes 	<ul style="list-style-type: none"> • « Geler » l'utilisation de vos données • Empêcher toute action sur vos données attente de l'exercice d'un de vos droits 	<ul style="list-style-type: none"> • S'opposer à l'utilisation de nos données pour un traitement précis • Justifier par « des raisons tenant à votre situation particulière »
Acteurs concernés 	Le responsable de traitement + Le sous-traitant		

	Droit à la portabilité	Droit à l'effacement
Définition et Objectif 	<ul style="list-style-type: none"> Récupérer les données que vous avez fournies à la plateforme Transférer ces données d'une plateforme à l'autre <p><u>Remarque</u> : Les données sont dans un format lisible par la machine.</p>	<ul style="list-style-type: none"> Effacer ou déréférencer des données personnelles vous concernant <p><u>Exemples</u> : photos ou liens gênants</p> <p><u>Remarque</u> : ce droit ne s'applique que dans certaines situations. Pensez à vous renseigner avant de faire la demande</p>
Acteurs concernés 	Le responsable de traitement	Le responsable de traitement + Les sous-traitants

Droit à la notification des failles de sécurité



Dans les textes :

Si la faille de sécurité peut entraîner un risque élevé pour les droits et libertés de la personne concernée, alors il l'informe :

- De l'existence de la faille ;
- Des données concernées ;
- Des conséquences possibles ;
- Des mesures prises et à prendre pour limiter les répercussions.



Dans la pratique :



OU



« Nous avons fait l'objet d'une faille de sécurité concernant vos données personnelles. Ce n'est pas très grave mais veuillez changer votre mot de passe svp »

III. Les organes de contrôle, les recours et les sanctions

✉ « par qui »

Délégué à la Protection des Données personnelles (DPD)



Qui est-ce ?

- Personne avec des compétences sur le droit à la protection des données et/ou informatique ;
- Interne ou externe à l'entreprise ;

Que fait-il ?

- Veille à la conformité des traitements de l'entreprise ;
- Point de contact des personnes concernées et de la CNIL ;
- Conseille le responsable de traitement, le sous-traitant mais aussi leurs employés ;

Les Autorité de Contrôle Indépendantes

Au moins une par état membre. En France, la



- **Informe** les acteurs de leurs obligations (mission de sensibilisation) ;
- **Conseille** les acteurs sur la façon de remplir leurs obligations ;
- **Reçoit les plaintes** des individus en rapport avec la réglementation des données personnelles ;
- **Contrôle** les acteurs qui traitent des données personnelles
- **Sanctionne** en cas de non-conformité

Autres organes de contrôle

Le Contrôleur Européen de la Protection des Données (EDPS)

Autorité de contrôle indépendante des institutions européennes (par exemple la Commission européenne) sur la protection des données

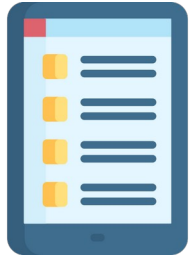
Comité Européen de la Protection des Données (EDPB)

Comprend :

- les chefs des autorités de l'autorité de contrôle de chaque État membre, ou leurs représentants.
- le Contrôleur européen de la protection des données, ou leurs représentants.

Veille notamment à la cohérence des pratiques et des sanctions des autorités

Recours possibles



- Recours devant une autorité de contrôle (dépôt de plainte en ligne sur le site de la CNIL)

- Recours judiciaire

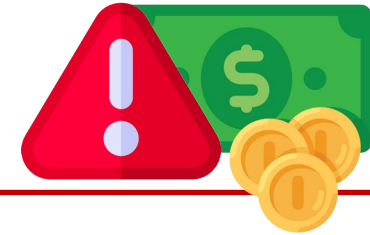


- Sanction administrative
- Sanction judiciaire



Sanctions possibles

- Rappel à l'ordre
- Injonction de mise en conformité (astreinte possible)
- Suspendre ou arrêter le traitement
- Impact sur l'image de l'entreprise
- Amende administrative
- Sanctions pénales



Montant maximum de l'amende :
20M € ou 4% du CA mondial

Exemples d'amendes administratives France

Déc
2018



Sécurité des données des
clients insuffisante



400.000 €

Nov
2020



Manquement à la sécurité +
Durée de conservation

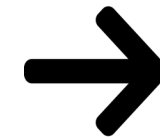


400.000 €
(1% CA)

Jan
2019



Manque de transparence +
Obligation d'information + Absence
de consentement pour la publicité



50.000.000 €

Déc
2021



150.000.000 €

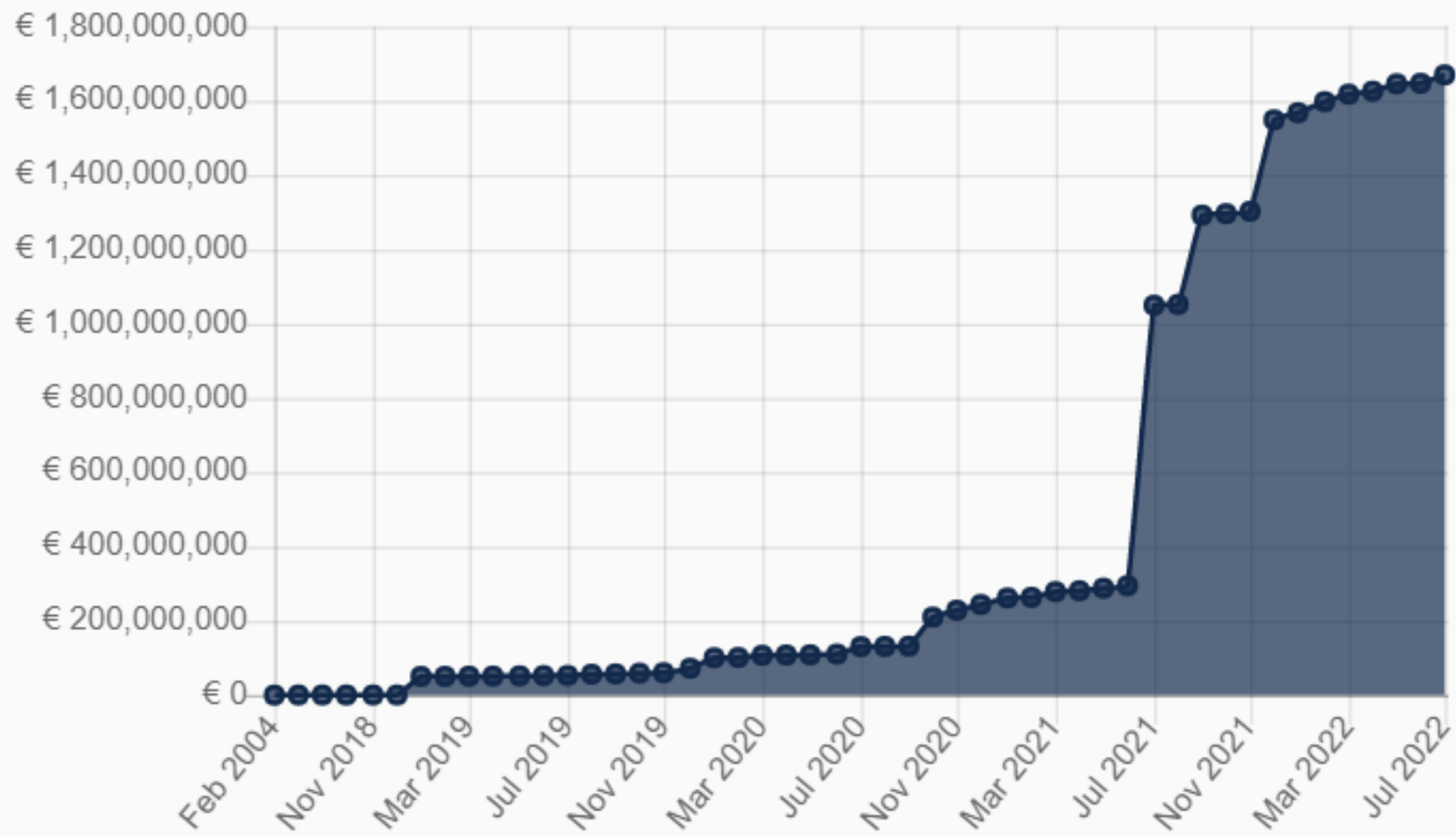
Statistics: Highest individual fines (Top 10)

The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

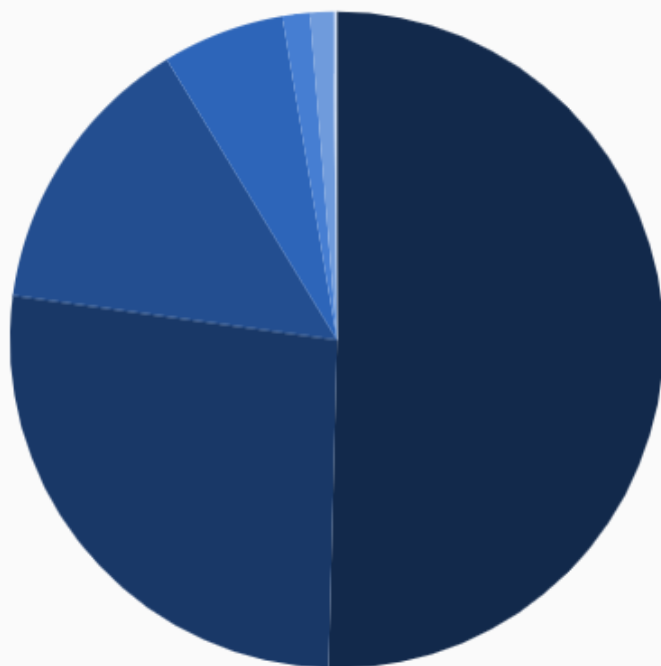
	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000	Non-compliance with general data processing principles	16 Jul 2021
2	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225,000,000	Insufficient fulfilment of information obligations	02 Sep 2021
3	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90,000,000	Insufficient legal basis for data processing	31 Dec 2021
4	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000	Insufficient legal basis for data processing	31 Dec 2021
5	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000	Insufficient legal basis for data processing	31 Dec 2021
6	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
7	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
8	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
9	Enel Energia S.p.A	Transportation and Energy	ITALY	26,500,000	Insufficient legal basis for data processing	16 Dec 2021
10	British Airways	Transportation and Energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational measures to ensure information security	16 Oct 2020

([Source](#))

a) Course of overall sum of fines (cumulative):



1. By total sum of fines:



Violation	Sum of Fines
Non-compliance with general data processing principles	€ 845,340,974 (at 271 fines)
Insufficient legal basis for data processing	€ 448,438,731 (at 415 fines)
Insufficient fulfilment of information obligations	€ 236,929,375 (at 107 fines)
Insufficient technical and organisational measures to ensure information security	€ 101,221,919 (at 235 fines)
Unknown	€ 22,729,400 (at 8 fines)
Insufficient fulfilment of data subjects rights	€ 18,788,370 (at 112 fines)
Insufficient fulfilment of data breach notification obligations	€ 1,495,041 (at 24 fines)
Insufficient data processing agreement	€ 1,048,080 (at 8 fines)
Insufficient involvement of data protection officer	€ 350,600 (at 12 fines)
Insufficient cooperation with supervisory authority	€ 305,229 (at 54 fines)
Insufficient fulfilment of data subject rights	€ 89,000 (at 3 fines)

Des questions ?

