Formation RGPD

Creative Commons CC-BY-SA

RGPD: Un contexte historique

Creative Commons CC-BY-SA

Identité

- Chacun de nous se présente sous plusieurs apparences (Famille, Travail,...)
- L'**identité** est la manière dont une *entité* est réliée à ses *apparences*

Creative Commons CC-BY-SA

Sur Internet, ces identités sont perçues à travers trois ensembles de données:

- Ce que l'on déclare de soi (infos fournies à l'inscription)
- Ce que l'on montre de soi (ses actions après l'inscription)
- Ce que l'on peut connaître (traces que l'on laisse)

Creative Commons CC-BY-SA

La collecte

Cependant, la collecte existe depuis l'invention de l'administration.
Voir en France: Le Livret Ouvrier.

Ces données ont déjà pu être utilisées contre des personnes.

- Massacre de la Saint Barthélémy
- Pays-Bas deuxième guerre mondiale

Creative Commons CC-BY-SA

Le danger s'est accéléré ensuite:

- La numérotation des personnes (révolution industrielle)
- La mécanographie (traitement automatique de l'information)

Creative Commons CC-BY-SA

La Loi Informatique et Libertés

Du 6 janvier 1978

Création d'une loi garantissant le respect des droits humains face:

- Au fichage
- Au traitement automatique de l'information
- Au croisement de données (informatique)

Creative Commons CC-BY-SA

Article 1

> L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Creative Commons CC-BY-SA

Application de cette loi

- Création d'organes indépendants de l'exécutif et des administrations
- Création d'un modèle juridique original: les **autorités administratives indépendantes**
- Création de la CNIL en tant qu première autorité administrative indépendante

Liste de Autorités adsministratives indépendantes

Creative Commons CC-BY-SA

Convention n°108 du Conseil de l'Europe du 28 janvier 1981

47 états membres - Directive 95/46/CE

- Début d'harmonisation
- Tout pays membres de l'UE doit créer une autorité indépendante du pouvoir chargée d'assurer la mise en vigueur des dispositions législatives relatives à la potection des personnes physiquesà l'égard des traitements des données à caractère personnel

Creative Commons CC-BY-SA

La CNIL

Commision Nationale de l'Informatique et des Libertés

https://www.cnil.fr

Creative Commons CC-BY-SA

Missions d'une autorité comme la CNIL

- Autorisation
- Contrôle
- Sanction
- Conseil

Creative Commons CC-BY-SA

Autorisation

- Étude de projets de traitements soumis à autorisation
- Élaboration de doctrines relatives aux différents types de traitement

Creative Commons CC-BY-SA

Contrôle

- Contrôles en ligne depuis 2014 (il fallait se rendre sur place avant)
- Mise en demeure pouvant être publique

Creative Commons CC-BY-SA

Sanction

- Tribunal administratif spécialisé au sein de la CNIL en matière de données personnelles
- Conseil d'État en cas d'appel

Creative Commons CC-BY-SA

Conseil

Tout le monde peut demander de l'aide et des informations à la CNIL

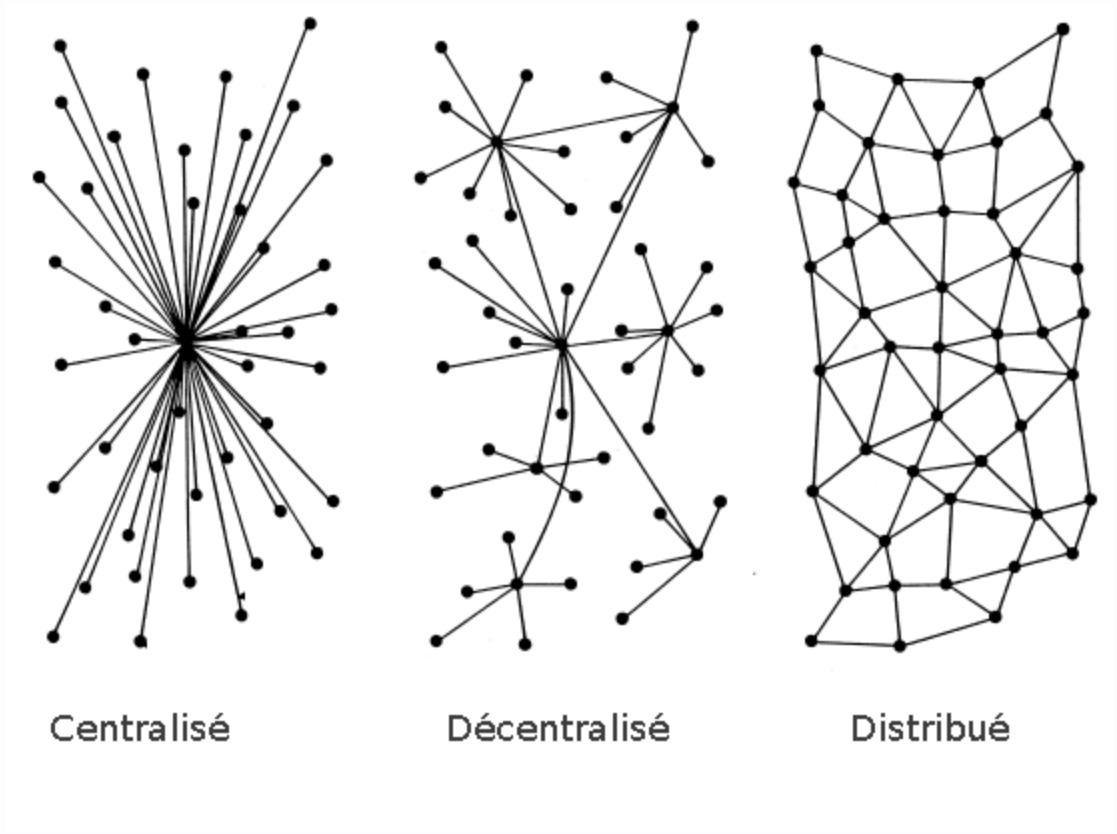
Site de la CNIL

Creative Commons CC-BY-SA

Internet

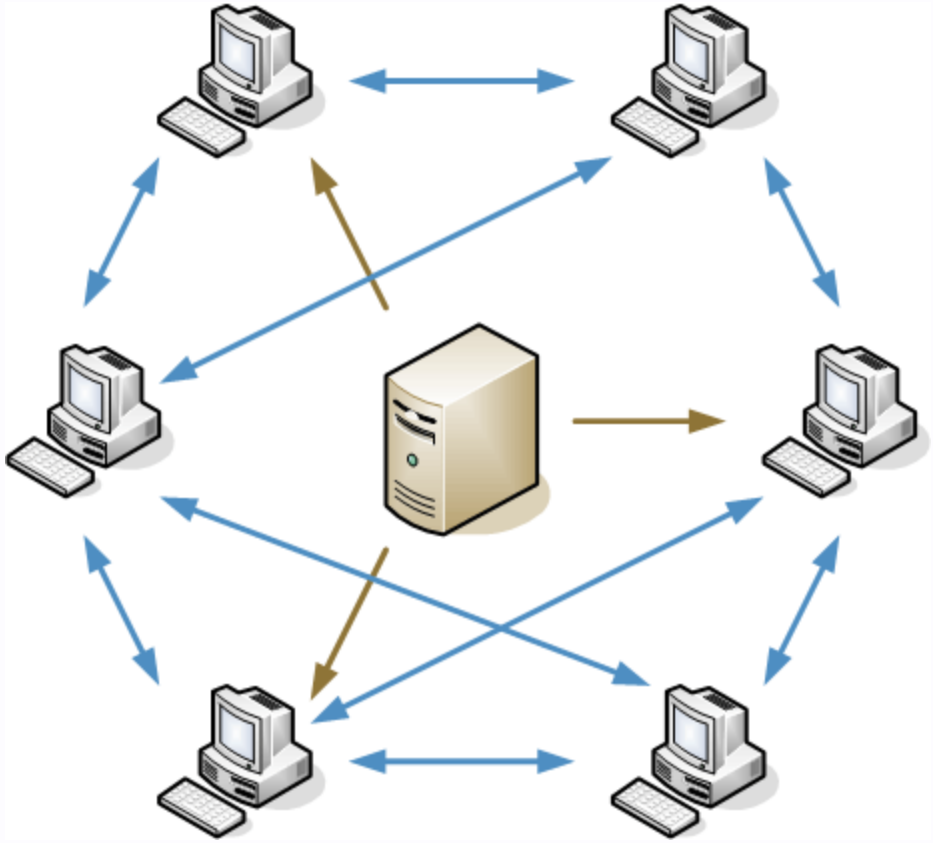
Creative Commons CC-BY-SA

Réseaux de communication



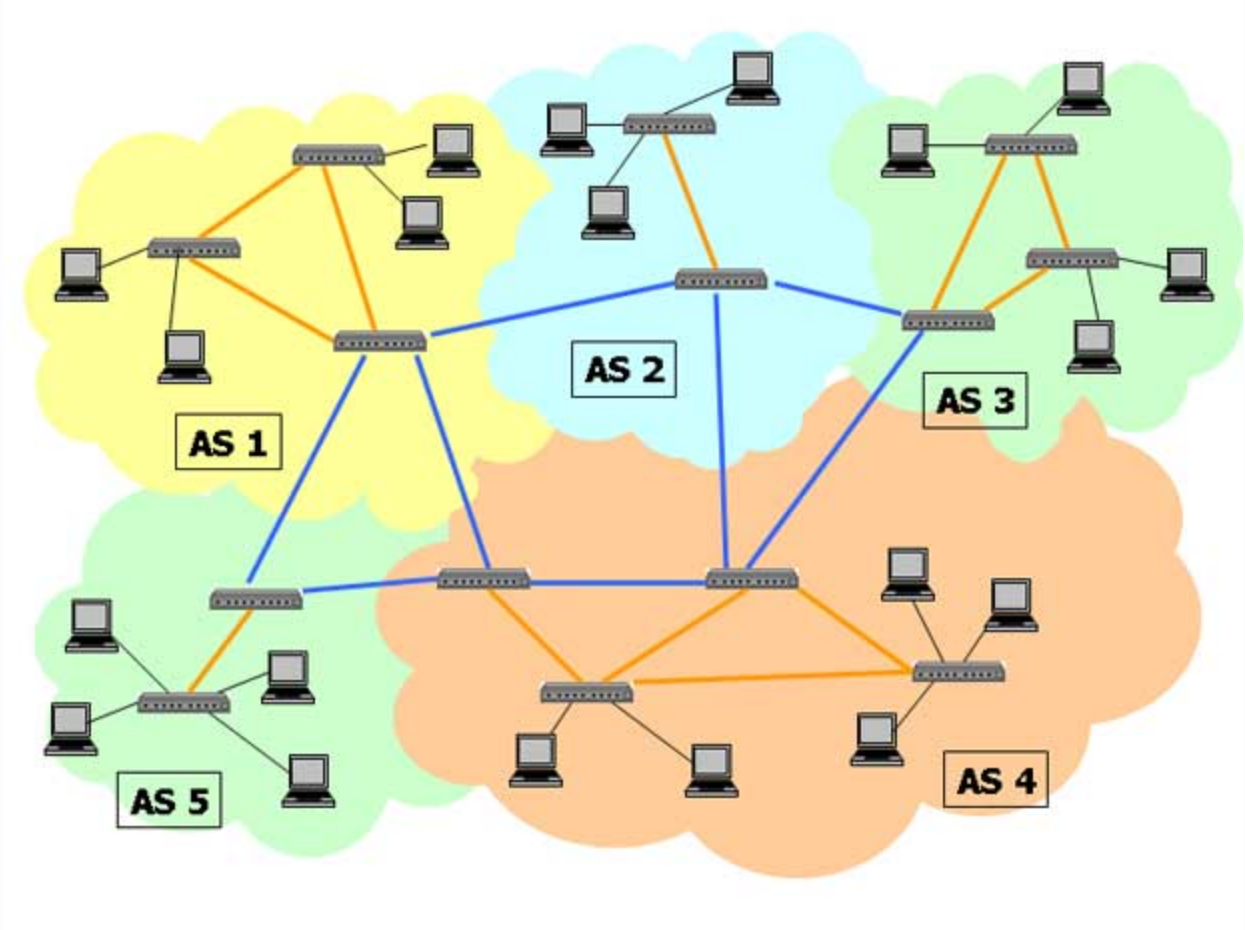
Creative Commons CC-BY-SA

Client / Serveur

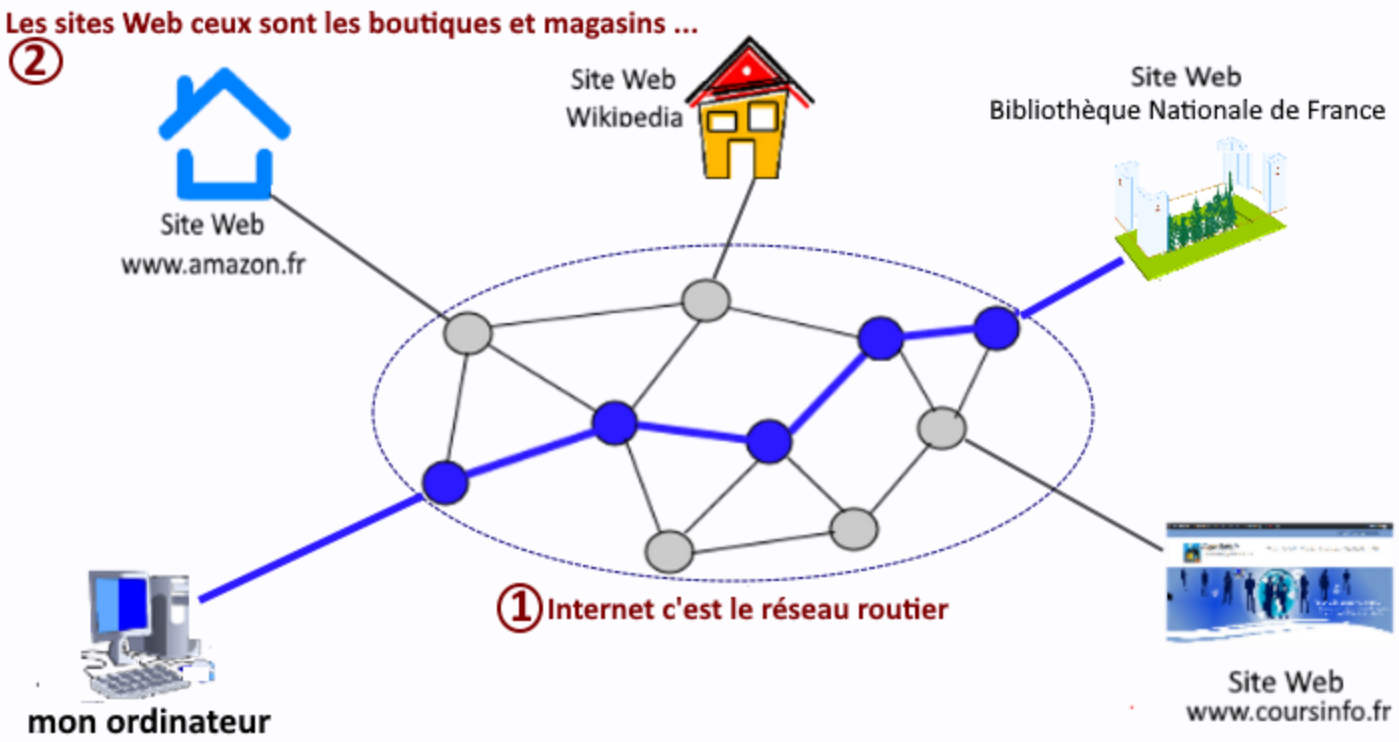


Creative Commons CC-BY-SA

L'intelligence est en périphérie



Creative Commons CC-BY-SA



CC coursinfo.fr

Creative Commons CC-BY-SA

Paquets



Creative Commons CC-BY-SA

Protocoles

- **Transport**: IP, TCP, UDP,...
- **Applications**: HTTP, SMTP, ...

Creative Commons CC-BY-SA

Le Web



Creative Commons CC-BY-SA

Le **World Wide Web**, ou "Toile", est un système hypertexte public fonctionnant sur Internet. Le web permet, grâce à un navigateur, de consulter des pages accessibles sur des sites.

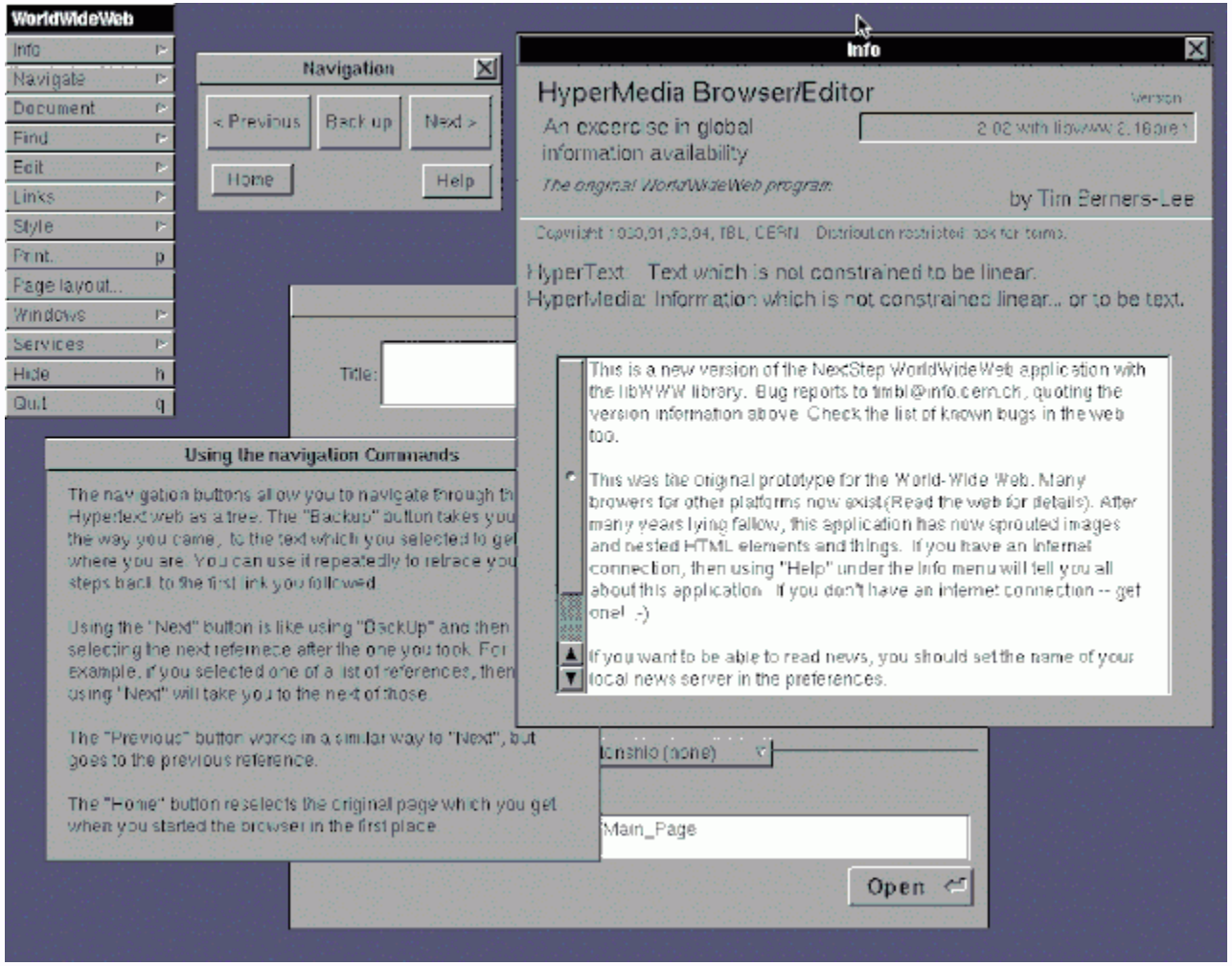
Creative Commons CC-BY-SA

Le Web a été créé en 1990 par Tim Berners-Lee, chercheur au CERN qui a cherché un nouveau système de partage de documents informatiques.

Première page web mise en ligne

Creative Commons CC-BY-SA

Premier navigateur web:



Creative Commons CC-BY-SA

Les traces laissées sur le web

Creative Commons CC-BY-SA

Les logs

```
147.X - [31/Oct/2019:01:30:41 +0100] "GET / HTTP/1.1" 301 232 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.1) Gecko/20100122 firefox/3.6.1"
188.X - [31/Oct/2019:02:39:58 +0100] "GET / HTTP/1.1" 301 232 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36"
188.X - [31/Oct/2019:02:40:32 +0100] "GET /contact.html HTTP/1.1" 301 244 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.70 Safari/537.36"
54.X - [31/Oct/2019:03:48:05 +0100] "GET / HTTP/1.1" 301 232 "-" "Go-http-client/1.1"
157.X - [31/Oct/2019:04:02:30 +0100] "GET /robots.txt HTTP/1.1" 301 242 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
158.X - [31/Oct/2019:08:43:26 +0100] "GET / HTTP/1.1" 301 232 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36"
90.X - [31/Oct/2019:13:02:26 +0100] "GET / HTTP/1.1" 301 236 "-" "Mail/3445.9.1 CFNetwork/902.3.1 Darwin/17.7.0 (x86_64)"
90.X - [31/Oct/2019:13:02:26 +0100] "GET / HTTP/1.1" 301 232 "-" "Mail/3445.9.1 CFNetwork/902.3.1 Darwin/17.7.0 (x86_64)"
34.X - [31/Oct/2019:13:04:11 +0100] "GET / HTTP/1.1" 301 232 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36"
54.X - [31/Oct/2019:13:09:21 +0100] "GET / HTTP/1.1" 301 236 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36"
213.X - [31/Oct/2019:22:34:36 +0100] "GET /?cprotect=2 HTTP/1.1" 301 243 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36"
109.X - [31/Oct/2019:22:46:28 +0100] "GET / HTTP/1.1" 301 232 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0"
```

Creative Commons CC-BY-SA

Les cookies



- Rester authentifié sur un site web (session)
- Peut contenir n'importe quoi
- Peut être lu par d'autres sites web (annonceurs, ...)

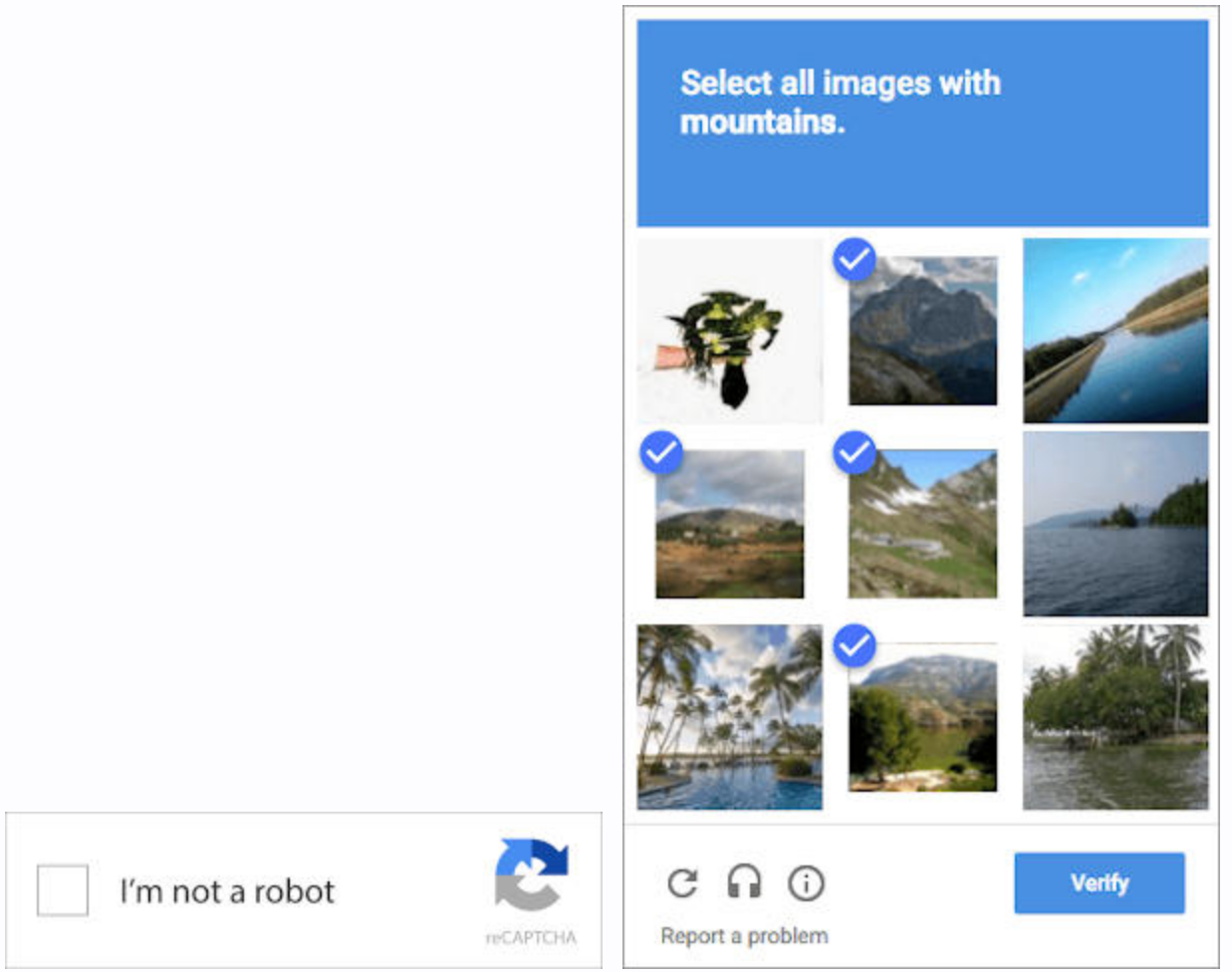
Creative Commons CC-BY-SA

Javascript



- Langage de programmation web
- Peut enregistrer les mouvements de souris, scroll,...

Creative Commons CC-BY-SA



Creative Commons CC-BY-SA

Autres moyens de récolter des données

- CDN (Content Delivery Network)
- Traqueurs de réseaux sociaux
- Métadonnées

Firefox 70 offre une protection renforcée contre le pistage. Voir également l'extension Lightbeam (qui n'est plus prise en charge)

Creative Commons CC-BY-SA

Le cloud

Le mythe:



Creative Commons CC-BY-SA

La réalité:



Digital Beijing, Beijing, China

Creative Commons CC-BY-SA



The Apple data center in Maiden, North Carolina.

Creative Commons CC-BY-SA



An aerial photograph of one of Amazon's data centers near Dulles International Airport in northern Virginia. (CJ photo by Don Carrington)

Creative Commons CC-BY-SA

Le cloud est un modèle de services en grande expansion.

Creative Commons CC-BY-SA

Les GAFAM

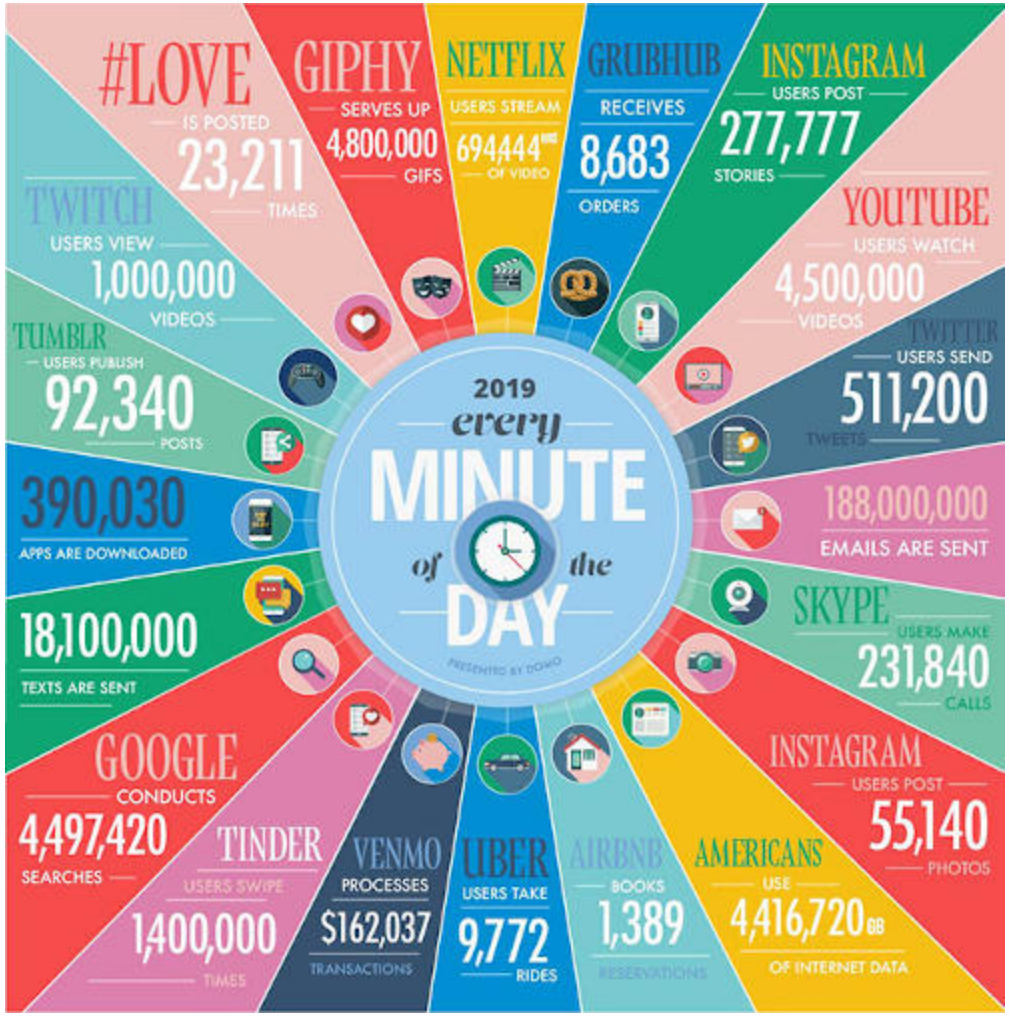


Creative Commons CC-BY-SA

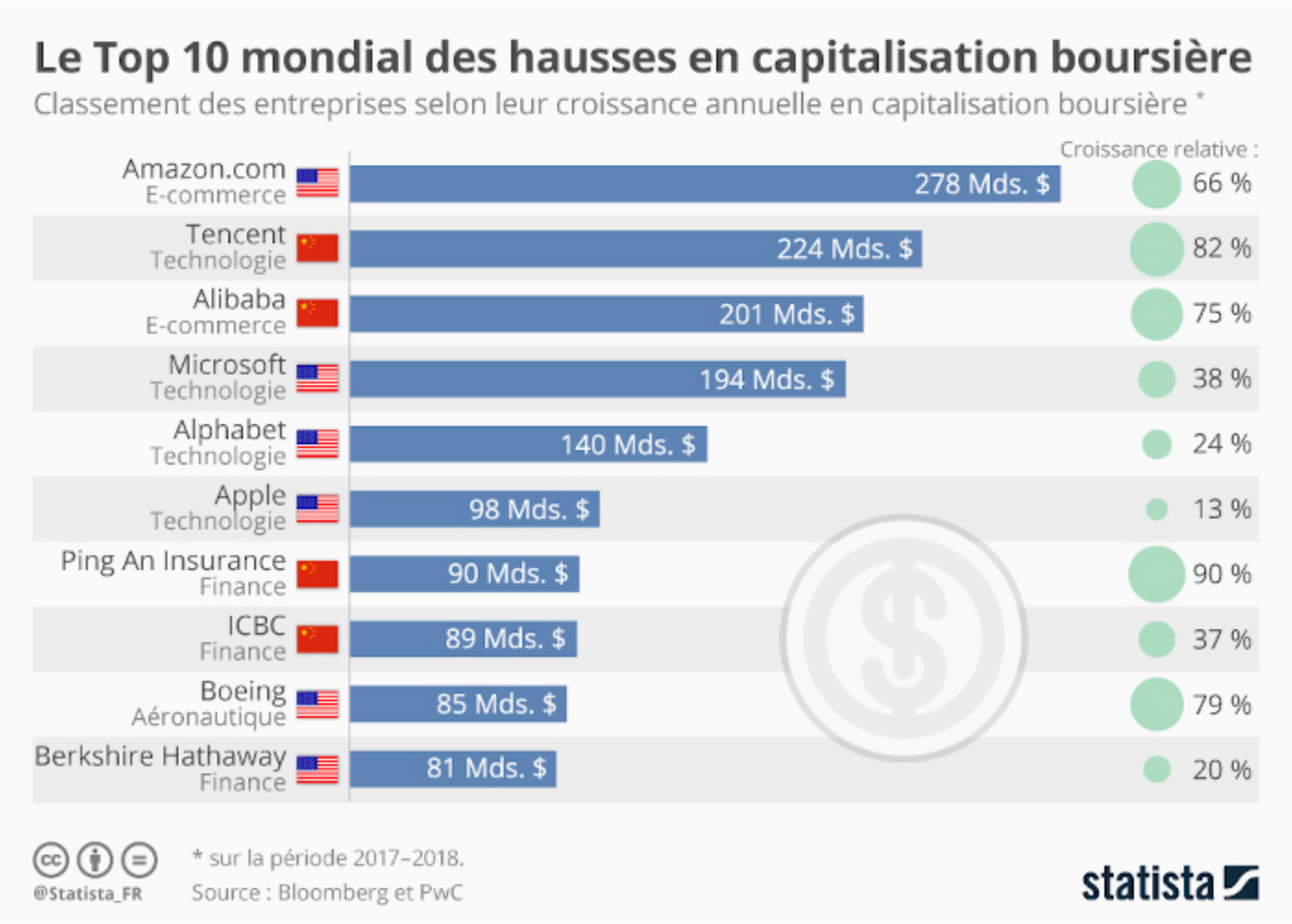
Re-centralisation

- Hégémonie du web
- Services "gratuits"
- Se rendre indispensable

Creative Commons CC-BY-SA



Creative Commons CC-BY-SA



Creative Commons CC-BY-SA

Compagnie	Employés	Chiffre d'Affaire	Bénéfices	Capitaux propres
Google (Alphabet)	103 000	136	39	177
Amazon	647 500	233	10	43
Facebook	39 500	56	22	84
Apple	132 000	266	59	107
Microsoft	144 000	125	39	102

en milliards de dollars (2018-2019)

Creative Commons CC-BY-SA

Google

- Modèle de la *régie publicitaire*

Rachats:



Creative Commons CC-BY-SA

Filiales d'Alphabet

Filiale	Domaine d'activité	Ancien nom
Calico	Biotechnlogies et transhumanisme	
DeepMind	Intelligence artificielle	
GV	Fond de placement	Google Ventures
Nest Labs	Domotique	
Verily	Recherche sur les sciences de la vie	Google Life Sciences
Waymo	Voiture autonome	Google Car
X	Robotique et Intelligence artificielle	Google X Lab

Creative Commons CC-BY-SA

Amazon

- 158 colis / seconde
- 14 millions / jour
- 5 milliards / an

Rachats:



... 101

Creative Commons CC-BY-SA

Amazon Web Services

- Le tiers de l'infrastructure *cloud* mondiale en 2016

Creative Commons CC-BY-SA

Jeff Bezos



154 milliards de dollars

Creative Commons CC-BY-SA

Facebook

- modèle de la *régie publicitaire*

Par jour:

- 1,3 milliards de personnes connectées
- 200 millions de photos mises en ligne

Rachats:







... 53

Un utilisateur de Facebook génère 95$ / an

Creative Commons CC-BY-SA

Voir la vidéo **3 minutes pour comprendre: ce que Facebook connaît de nous**

Creative Commons CC-BY-SA

Apple

- Vente de matériel
- Contenu édité par des tiers mais téléchargeable sur une plateforme Apple (iTunes)

Rachats: 90 entreprises

Creative Commons CC-BY-SA

Microsoft

Rachats:



... 236

Creative Commons CC-BY-SA

"Et alors? Je n'ai rien à cacher..."

Creative Commons CC-BY-SA

Nothing to Hide: 9:20 --> 19:09

Creative Commons CC-BY-SA

Vidéo Quadrature du Net: **Nos données ne sont pas des marchandises**

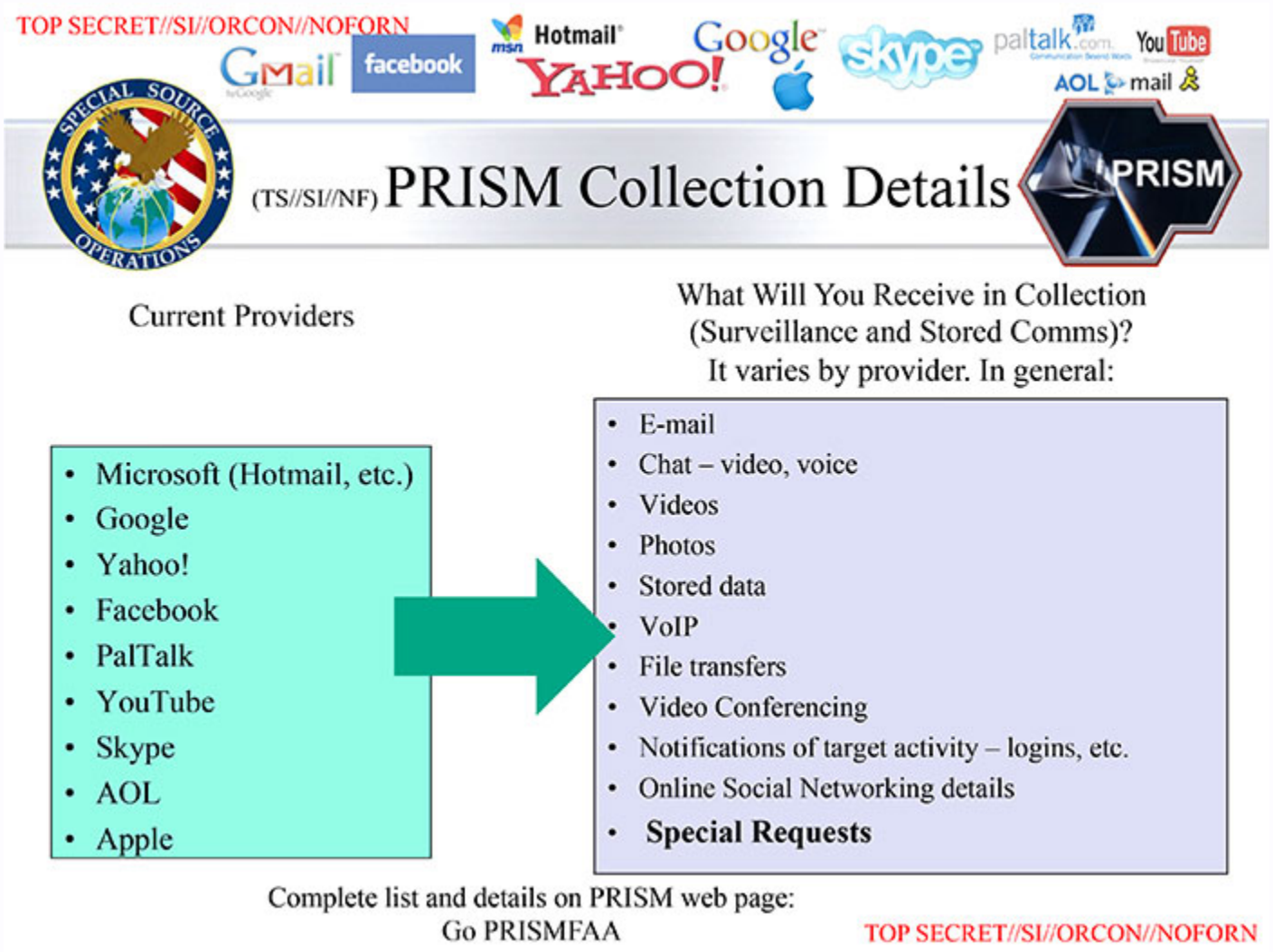
Creative Commons CC-BY-SA

Révélations Snowden



Creative Commons CC-BY-SA

PRISM



Creative Commons CC-BY-SA

Serveurs PRISM de la NSA dans l'Utah



Creative Commons CC-BY-SA

Affaire Cambridge Analytica

- Application tierce installée par plusieurs centaines de milliers d'utilisateur Facebook
- Accès aux données de l'utilisateur "à des fins de recherche"
- Par connexion, 87 millions de personnes concernées
- Données analysées et vendues à l'équipe de campagne de Donald Trump

Creative Commons CC-BY-SA

En France: projet Alicem

- Application mobile de reconnaissance faciale
- Connexion aux services publics en ligne (type FranceConnect)

Creative Commons CC-BY-SA

Que peut-on faire ?

Creative Commons CC-BY-SA

Vidéo: Reclaim our Privacy

Creative Commons CC-BY-SA

RGPD

Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des **personnes physiques** à l'égard du **traitement** des **données à caractère personnel** et à la **libre circulation de ces données**

- Concerne les données à caractère personnel
- Leur traitement / Circulation
- Données ratachées à des personnes physiques (et non des groupes)

Creative Commons CC-BY-SA

Directive européenne	Règlement européen
Donne des objectifs à atteindre par les pays membres, avec un délai. Ce délai permet aux gouvernements nationaux de s'adapter à la nouvelle réglementation.	Directement applicable sans aucune mesure de transcription nationale. On dit qu'il est d'application immédiate ou d'effet direct

Creative Commons CC-BY-SA

Données à caractère personnel?

Vidéo Quadrature du Net

Creative Commons CC-BY-SA

Champ d'application

Ne concerne uniquement les **personnes physiques**. La loi *Informatique et Libertés* ne s'applique pas aux entreprises.

Creative Commons CC-BY-SA

Définitions

L'article 4 du RGPD définit bien les choses tout en étant synthétique.

Aux fins du présent règlement, on entend par:

Creative Commons CC-BY-SA

« «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement **ou indirectement** *, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »

*Exemple des *spaghettis*, *macaronnis* ou *semoule*

Creative Commons CC-BY-SA

> «traitement», 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, 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;

Creative Commons CC-BY-SA

Interdiction du traitement des "données sensibles"

Voir l'article 9 du RGPD.

> Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

Creative Commons CC-BY-SA

Critères de licéité

Creative Commons CC-BY-SA

Finalité

Elle doit être:

- **Déterminée**: Pourquoi ces données sont collectées
- **Explicite**: Clairement affichée
- **Légitime**: Pour de bonnes raisons (voir les 6 bases légales de la CNIL)

Voir la page Finalité d'un traitement

Creative Commons CC-BY-SA

Responsable de traitement

Un responsable du traitement doit être désigné. Il a des obligations à tenir. Une personne fonitonnellement indépendante de la hiérarchie, doit mettre en place les moyens nécessaires au bon déroulement des traitements.

Voir la page DPO

Creative Commons CC-BY-SA

Destinataires des données traitées

Est-ce que ces données sont transmises? Si oui, à qui et pourquoi?

Creative Commons CC-BY-SA

Mesures de sécurité de conservation

Quelle sécurité est mise en place pour sécuriser ces données?

*Différence entre obligation de **résultat** et obligation de **moyens**.*

Creative Commons CC-BY-SA

Exercice des droits des personnes

Les personnes concernées doivent pouvoir exercer leurs droits sur ces données.

- Information
- Accès
- Rectification
- Opposition
- …

Creative Commons CC-BY-SA

Bases légales

Un traitement de données à caractère personnel, pour être licite, doit respecter l'une des six bases légales fixées par le RGPD. Ce règlement reprend quasiment à l'identique les 6 bases légales de traitement déjà listées au sein de la Directive 95/46/CE.

Voir l'article 6 du RGPD.

Creative Commons CC-BY-SA

Consentement explicite de la personne

Le consentement doit être **univoque**, **libre**, **spécifique** et **éclairé**.

Creative Commons CC-BY-SA

Nécessité pour l'exécution d'un contrat

Exemples:

- Traitement de l'adresse postale d'un client pour l'envoi de produits achetés en ligne.
- Traitement des données des salariés pour que l'employeur puisse précdéder à la paye de ces derniers.

Creative Commons CC-BY-SA

Respect d'une obligation légale

Exemples:

- Traitement des données relatives aux rémunérations des employés (numéro de sécurité sociale, ...)

Creative Commons CC-BY-SA

Sauvegardes des intérêtes vitaux de la personne

Exemples:

- Traitement de données à des fins humanitaires

Creative Commons CC-BY-SA

Mission d'intérêt public

ou relevant de l'autorité publique dont est investi le responsable

Exemples:

- Centre sociaux-culturels?

Creative Commons CC-BY-SA

Intérêts légitimes

poursuivis par le responsable de traitement ou par un tiers, **mis en balance** avec l'intérêt légitime de la personne.

Exemple:

- Lecture du mail pour le classer comme SPAM

Creative Commons CC-BY-SA

Obligations du responsable de traitements



Creative Commons CC-BY-SA

Tenir un registre des traitements

Le registre doit décrire de façon suffisamment détaillée la façon dont sont traitées les données. **C'est un bon moyen de se demander si toutes les données récoltées sont vraiment utiles.**

Voir la page Registre des activités de traitement

Creative Commons CC-BY-SA

Réaliser une analyse d'impact

Lorsqu’un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Comment savoir si c'est nécessaire?

PIA,logiciel pour aider à réaliser une AIPD

Creative Commons CC-BY-SA

Encadrement des transferts hors UE

Impossible d'envoyer les données dans des espaces politiques où les données à caractère personnel ne sont pas respectées)

Voir la page Transférer des données hors UE

Creative Commons CC-BY-SA

Information des personnes concernées

Détails

Creative Commons CC-BY-SA

Procédures en cas de violation de données

Voir la page Notifier une violation de données personnelles

Creative Commons CC-BY-SA

Évolutions du fait du RGPD

Creative Commons CC-BY-SA

Principales dispositions

Creative Commons CC-BY-SA

Passage d'un régime d'autorisation à un régime répressif

Creative Commons CC-BY-SA

Cadre du RGPD harmonisé au sein de l'Union européenne

Creative Commons CC-BY-SA

renforcement du consentement

Il doit être **explicite** de la part de la personne.

Creative Commons CC-BY-SA

Droit à la portabilité des données

Un organisme traitant des données à caractère personnel doit prévoir un moyen possible pour l'utilisateur de récupérer ses données. (Ouverture à la concurrence)

Creative Commons CC-BY-SA

Protection intégrée de la vie privée

Obligation de **minimisation** des données. Uniquement celles qui sont nécessaires, de la façon dont il est strictemetn nécessaire.

Creative Commons CC-BY-SA

Obligation de notification en cas de violation

Obligation du responsable de traitement d'informer l'autorité et les personnes concernées en cas de violation. (erreur ≠ faute)

Creative Commons CC-BY-SA

Mise en pratique

Creative Commons CC-BY-SA

Registre des traitements

Il est obligatoire que le responsable des traitements tienne une **registre des traitements** à jour. Ce registre doit renseigner:

Creative Commons CC-BY-SA

- Les **parties prenantes** (représentants, sous-traitants, co-responsables, etc. qui interviennent dans le traitement des données)
- Les **catégories** de données traitées
- **À quoi** servent ces données (ce que vous en faites)
- **Qui** accède à ces données
- **À qui** elles sont communiquées
- **Comment** sont-elles **sécurisées**

Exemple

Creative Commons CC-BY-SA

Information des personnes concernées et transparence

Le règlement général sur la protection des données (RGPD) impose une information concise, transparente, compréhensible et aisément accessible des personnes concernées. Les informations à donner sont:

Creative Commons CC-BY-SA

- **Identité** et **coordonnées de l'organisme** (responsable du traitement)
- **Finalités** du traitement
- **Base légale** du traitement (ce qui donne le droit d'effectuer un traitement)
- Caractère **obligatoire** ou **facultatif** du recueil des données et **conséquences** pour la personne en cas de non-fourniture des données

Creative Commons CC-BY-SA

- **Destinataires** ou **catégories de destinataires** s'il y a (y compris les sous-traitants)
- **Droits** des personnes concernées (accès, rectification, rectification, effacement doivent être applicables pour tous les traitements)
- **Cordonnées** du délégué à la protection des données de l'organisme
- Droit d'introduire une **réclamation auprès de la CNIL**

Creative Commons CC-BY-SA

Voir la page concernée sur le site de la CNIL.

Consulter les exemples.

Creative Commons CC-BY-SA

Ressources

Creative Commons CC-BY-SA

- CNIL: RGPD: par où commencer
- Les fichiers des associations en question

Creative Commons CC-BY-SA