

# Droits et devoirs dans l'utilisation des données

Aurore Blot – GRTgaz  
[aurore.blot@insa-rouen.fr](mailto:aurore.blot@insa-rouen.fr)

# Donnée personnelle / Donnée sensible



# QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?



- › Toute information qui
  1. permet d'identifier une personne physique ou
  2. se rapporte à une personne physique identifiée ou identifiable

- › Identification directe

*Nom, prénom, adresse*

- › Ou identification indirecte

*Numéro de compte, numéros de tél., adresse IP, situation familiale, âge...*

- › À partir d'une donnée unique

*Numéro de contrat, identifiant...*

- › Ou à partir d'un croisement de données

*Date et lieu de naissance, célibataire, emprunteur, primo accédant...*

# QU'EST-CE QU'UNE DONNÉE SENSIBLE ?



- › C'est une donnée personnelle de type :
  - Données à caractère personnel
  - Données de santé
  - Certaines données industrielles

## Liste non exhaustive

- › la santé,
- › le numéro d'identification national unique  
*(NIR pour la France = numéro de sécurité sociale).*
- › l'origine raciale ou ethnique,
- › les opinions politiques,
- › les convictions religieuses ou philosophiques,
- › l'appartenance syndicale,
- › les données génétiques,
- › les données biométriques aux fins d'identifier une personne physique de manière unique,
- › la vie sexuelle ou l'orientation sexuelle,
- › des condamnations pénales ou infractions...

# QU'EST-CE QU'UN TRAITEMENT DE DONNÉE PERSONNELLE ?



- › Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire qu'on ne peut pas collecter ou traiter des données personnelles simplement au cas où cela serait utile un jour.
- › A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle.
  
- › Exemple - Traitement de données personnelles
  - Tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.
  
- › Exemple - Non traitement de données personnelles
  - Un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « [compagnieA@email.fr](mailto:compagnieA@email.fr) »).

Que vise la réglementation ?



# LOI INFORMATIQUE ET LIBERTE

6 JANVIER 1978



- › Base de données = recueil d'informations électroniques ou non
- › Traiter en masse des données, de manière rapide et efficace
- › 1974 : Projet SAFARI (Système Automatisé pour les Fichiers Administratifs et Répertoires des Individus)
  - vise à centraliser les répertoires d'identification (régionaux), le fichier de la CNAV (retraite) et ceux de la carte d'identité
  - « *entrave grave à la liberté* »
  - Le Monde – 21 mars 1974

## 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

qui serait destiné à rassembler la masse énorme des renseignements gravés 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 doter chaque Français par un « identifiant », qui ne définit pas que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite

jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, 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 ministre de la justice, adressées 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

Rue Jules-François, à Paris-13<sup>e</sup>, dans des locaux du ministère de l'intérieur, un ordinateur Ibs 80 avec bi-processeur est en cours de mise en marche. A travers la France, les différents services de police distamment,

l'origine, budgétairement, n'ont pas du tout prévu pour la tâche qu'il a finalement assumée, mais pour « traiter » les données administratives du Fichier national des contributeurs (F.N.C.). Il s'agit donc apparemment d'un ordinateur de type Ibs 80.

Ce n'est pas, pourtant, que les avertissements aient manqué. Le Conseil d'Etat en 1975, puis le ministère de la justice en 1976 (qui avait rappelé le rôle gravé à l'autorité judiciaire de « gardien des libertés

publiques ») n'apparaît pas — sauf erreurs négligeables, relativement — que l'accès des tiers au droit à contrôler des personnes visées — par demande d'un extrait — ait jamais provoqué des bavures judiciaires.

de la commission. D'autant qu'il est d'ores et déjà connu que M. Touffan a été rayé de la liste des « sachants ». Il semble d'ailleurs que les recherches qui sont enregistrées portent moins sur le renouvellement des

d'un équipement technique, à illustrer son discours par un large reportage sur les équipements du tribunal de Bobigny — plus réduits, donc plus rapides à réaliser, ainsi plus vite source d'argent pour leurs

- › 6 janvier 1978 – Loi relative à l'informatique, aux fichiers et aux libertés
- › Protection de la vie privée des citoyens face aux moyens de traitement automatisés de données numériques

# RGPD

25 MAI 2018



- › Règlement Général sur la Protection des Données
  
- › RGPD remplace et complète la loi Informatique et Libertés dans le but de redonner aux personnes la maîtrise de leurs données personnelles.
  
- › Elle s'articule autour de 3 piliers :
  - Renforcement des droits des personnes
  - Responsabilisation des acteurs
  - Renforcement des sanctions
  
- › Mais elle n'a rien révolutionnée en matière de conservation des données :
  - La limitation des durées de conservation figure déjà dans la loi Informatique & Libertés de 1978. Ne pas être conforme à RGPD sur ce point revient, en réalité, à ne pas être conforme à la loi de 1978.



# QUI EST CONCERNÉ ?



- › Tout organisme quels que soit sa taille, son pays d'implémentation et son activité dès lors que :
  - Elle traite des données personnelles
  - Pour son compte ou non
  - Elle est établie sur le territoire de l'UE ou que son activité cible des résidents européens
  
- › Exemples de société éligible au RGPD
  - Société établie en France et ayant ses clients aux USA
  - Société établie en Australie proposant un site d'e-commerce en français livrant des produits en France.

# LA CNIL



› **Autorisation administrative indépendante française** créée par la loi du 6 janvier 1978

→ veiller à la protection des données à caractère personnel et de la vie privée

› **3 missions**

› **Information**

- Informe les autorités publiques, les professionnels et les citoyens des droits et des devoirs en matières de données personnelles.
- Permet aux citoyens d'exercer leur droit d'accès à certains fichiers (RG).
- Moyens utilisés : site internet (loi et modalités d'application), rapport annuel, publicité faite sur des délibérations (via la presse), organisation de réunions thématiques régionales

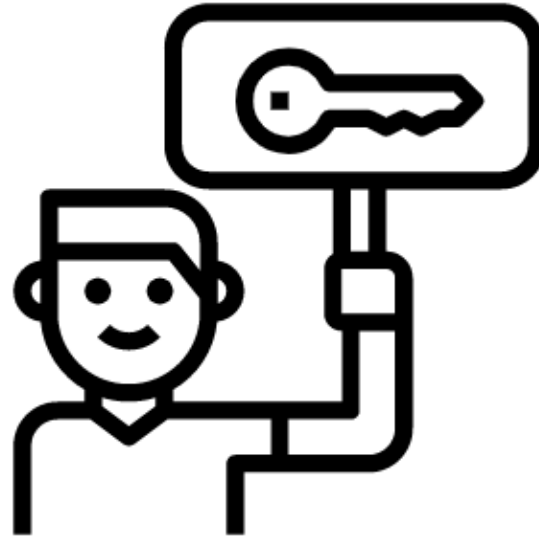
› **Contrôle**

- respect de la loi a priori (dossiers de déclaration) et a posteriori (visites dans les organismes).

› **Répression**

- avertissement, mise en demeure et sanction financière. Peut saisir le parquet dans des cas graves.

# Renforcement des droits personnels



# LE DROIT À L'INFORMATION



- › **Soyez curieux des informations vous concernant**
  
- › Toute personne a le droit de savoir si elle est fichée et dans quels fichiers.
  
- › Toute personne qui met en œuvre un fichier contenant des données personnelles doit renseigner les points suivants :
  - identité du responsable,
  - objectif de la collecte d'informations,
  - caractère obligatoire ou facultatif des réponses,
  - conséquences de l'absence de réponse,
  - destinataires des informations, ...
  
- › **Limite** : l'obligation d'information est alléger lorsque les données sont anonymisées et exclue pour les fichiers de police, de gendarmerie ou relatifs à des condamnations pénales.

# LE DROIT D'ACCÈS



- › Consultez vos données personnelles (complémentaire au droit d'informations)
- › Toute personne justifiant de son identité a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir une copie.
- › **Limite** : si le responsable estime que la demande est abusive ou si les données sont sous une forme ne présentant aucun risque, leur consultation est refusée : sécurité de l'État, la défense, la police ou la gendarmerie

# LE DROIT DE RECTIFICATION



- › Info ou intox, à vous de contrôler
- › Toute personne peut
  - faire rectifier, compléter, verrouiller ou effacer des informations qui la concernent
  - lorsque ont été décelées des erreurs ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.
- › Pour exercer son droit de rectification, il faut écrire à l'organisme qui détient les informations
- › Le demandeur peut obtenir gratuitement une copie de l'enregistrement modifié

# LE DROIT À LA LIMITATION



- › Geler l'utilisation de vos données
- › En cas d'inexactitude / opposition à ce que vos données soient traitées :
- › la loi autorise l'organisme à procéder à une vérification ou à examen de votre demande pendant un certain délai.
- › Pendant ce délai, vous avez la **possibilité de demander à l'organisme de geler l'utilisation de vos données.**
- › Concrètement, il ne devra plus utiliser les données mais devra les conserver.

# LE DROIT D'OPPOSITION



- › Restez maître de vos données personnelles
  
- › Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier et cela sans se justifier
  
- › Droit d'opposition :
  - refus de répondre lors d'une collecte non obligatoire de données,
  - refus de donner l'accord écrit obligatoire pour le traitement de données sensibles (opinions politiques ou religieuses),
  - demander la radiation des données contenues dans des fichiers commerciaux,
  - exiger la noncommercialisation d'informations
  
- › Limite : le droit d'opposition n'existe pas pour les services fiscaux, de police, de la justice, de la sécurité sociale...



# LE DROIT À LA PORTABILITÉ



- › Obtenez une copie réutilisable de vos données
- › Possibilité de récupérer une partie de vos données dans un format lisible par une machine.
- › Libre à vous de stocker ailleurs ces données portables ou les transmettre facilement d'un système à un autre, en vue d'une réutilisation à d'autres fins.
- › Complémentaire du droit d'accès
- › **Limite** : Ne s'applique que si vos données sont traitées de manière automatisée et sur la base de votre consentement préalable ou de l'exécution d'un contrat conclu avec vous.

# LE DROIT À L'OUBLI



- › Un droit à garder à l'esprit
- › La personne concernée a le droit d'obtenir du responsable du traitement l'effacement dans les meilleurs délais de données à caractère personnel la concernant.
- › Le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais lorsqu'un des motifs définis dans la réglementation s'applique.
- › Exemple de motifs
  - Fin de la finalité du traitement
  - Retrait du consentement de la personne
  - Traitement illicite
  - ...

# Responsabilisation des acteurs



# RESPONSABILISATION DES ACTEURS



- › Inverser la charge de la preuve
- › Les responsables de traitement devront être en mesure de prouver à tout moment et pour tout traitement qu'ils respectent le règlement
- › Les fichiers à risques doivent être déclarés à la CNIL.

# RESPONSABILISATION DES ACTEURS



## › Obligations

- › **La collecte des données** : consentement et sauf dérogation, pas de données sensibles.
- › **La finalité des traitements** : cohérence par rapport à un objectif. Pas de réutilisabilité pour un autre objectif.
- › **La durée de conservation des informations** : date de péremption raisonnable en fonction de l'objectif fixée par le responsable.
- › **La sécurité des fichiers** : mesures de sécurité physiques (sécurité des locaux) et logiques (sécurité des systèmes d'information)
- › **La confidentialité des données** : accès aux données seulement pour les destinataires explicitement désignés ou des « tiers autorisés » de façon ponctuelle et motivée (par ex. : la police, le fisc)

# Renforcement des sanctions



# SANCTIONS



- › Les acteurs sont tenus d'informer les autorités de toute violation de données dans les 72 heures suivant la date à laquelle elles en ont eu connaissance.
- › En cas de non-respect de cette réglementation, les firmes risquent une amende salée allant jusqu'à 4 % de leur chiffre d'affaires.
- › Près de 1,1 Milliards d'euros d'amendes liées au RGPD en Europe en 2021
- › Dont Amazon, WhatsApp, Google, ...

# EXEMPLES DE SANCTION (appels en cours)



- › **Amazon** : 746 Millions d'euros
- › **WhatsApp** : 225 Millions d'euros
- › Suspicion de partage de données à Facebook
  
- › **Google** : 50 Millions d'euros
  
- › **Disqus** : 2,5 Millions d'euros
- › Entreprise qui propose un plug-in de commentaires sur des sites.
- › L'entreprise s'est justifiée en expliquant ne pas savoir que le RGPD s'appliquait dans le pays.
  
- › **AG2R la Mondiale** : 1,75 Millions d'euros
- › Durée de conservation des données / Information des personnes
  
- › **Monsanto** : 400 000 euros
- › Suspicion de ne pas avoir informé les personnes dont les données étaient enregistrées dans un fichier dédié au lobbying