Informatique & Libertés

#SRETI

Benjamin Vialle
http://benjamin-vialle.net

École Centrale de Nantes, le 6 décembre 2013

Table des matières

Table des matières

Le projet SAFARI

- SAFARI : système automatisé pour les fichiers administratifs et le répertoire des individus
- Projet d'*interconnexion* des fichiers nominatifs de l'administration française, notamment par le biais du numéro INSEE [1]
- Révélation de ce projet, le 21 mars 1974 par le quotidien Le Monde, dans l'article intitulé « SAFARI ou la chasse aux Français » de Philippe Boucher [2]
- Crainte d'un fichage général de la population

1. Le numéro de sécurité sociale (nom usuel), ou numéro d'inscription au répertoire des personnes physiques (abrégé en NIRPP ou plus simplement NIR) est un code alphanumérique servant à identifier une personne dans le répertoire national d'identification des personnes physiques (RNIPP) géré par l'Insee

2. « SAFARI ou la chasse aux Français » paru dans le Monde

Le projet SAFARI

- Création d'une commission informatique et libertés pour proposer des mesures garantissant que l'informatique se développe dans le respect de la vie privée, des libertés individuelles et publiques.
- Cette "Commission Informatique et Libertés" proposa, après de larges consultations et débats, de créer une autorité indépendante.
- C'est ce que fit la loi du 6 janvier 1978 en instituant la *Commission nationale de l'informatique et des libertés*.
- Le projet SAFARI n'a finalement jamais vu le jour.

Bref rappel historique

1. La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et Libertés » [3]
2. Directive européenne 95/46 CE du 24 octobre 1995 pour la protection des personnes physiques à l'égard des traitements de données à caractère personnel [4]
3. La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : remaniement de la loi « Informatique et Libertés » [5]
4. Le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. 2005 [6]

3. Texte de la loi n° 78-17 du 6 janvier 1978 sur Legifrance (version en vigueur)
4. Texte de la directive européenne 95/46 CE du 24 octobre 1995 sur EurLex
5. Texte de la loi n° 2004-801 du 6 août 2004 sur Legifrance
6. Texte du décret n° 2005-1309 du 20 octobre 2005 sur Legifrance

La Commission Nationale de l'Informatique et des Libertés

- Première autorité administrative indépendante française
- Collège de 17 membres siégeant en formation plénière ou restreinte (6 membres)
- Plus d'informations sur www.cnil.fr

Missions de la CNIL

- Mission d'information : informe les personnes concernées et les responsables de traitements de leurs droits et obligations.
- Mission de contrôle : veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément à la loi.
- Mission de conseil :donne un avis sur la conformité à la loi des projets qui lui sont soumis.
- Mission de veille : anticiper les évolutions sociétales, économiques et technologiques pouvant avoir un impact sur la protection des données.

Loi Informatique et Libertés

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.*

Donnée à caractère personnel

Article 2

Constitue une donnée à caractère personnel ***toute information relative à une personne physique identifiée ou qui peut être identifiée****, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.*

Données à caractère personnel

- nom, prénom, date de naissance ;
- adresse postale ou électronique ;
- adresse IP ;
- numéro de carte de paiement ;
- plaque d'immatriculation d'un véhicule ;
- photo ;
- numéro de téléphone ;
- numéro de sécurité sociale ;
- ...

Données à caractère personnel

Mais aussi

- cookies qui permettent de reconnaître des visites antérieures ;
- informations PNR[7] (*Passenger Name record*) ;
- empreinte digitale ;
- ADN ;
- données médicales, génétiques et biométriques.

7. Données des dossiers passagers : Un PNR est, au départ, l'enregistrement dans une base de données des informations qu'une compagnie aérienne juge nécessaires pour établir une réservation de vol. Il contient, notamment, sur le passager, son nom, sont itinéraire, les informations pour contacter l'un des participants du voyage, les réservations, les informations de tickets et les préférences pour les passagers, par exemple les repas pendant les vols (végétariens, kasher, etc.)

Donnée à caractère personnel

Article 2

*[. . .]Pour déterminer si **une personne est identifiable**, il convient de considérer l'**ensemble des moyens en vue de permettre son identification** dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.[. . .]*

Traitement de données à caractère personnel

Article 2

[. . .]Constitue un traitement de données à caractère personnel toute opération [. . .] portant sur de telles données [. . .] et notamment la ***collecte****, l'****enregistrement****, l'****organisation****, la* ***conservation****, l'****adaptation*** *ou la* ***modification****, l'****extraction****, la* ***consultation****, l'****utilisation****, la* ***communication*** *par transmission, diffusion ou toute autre forme de mise à disposition, le* ***rapprochement*** *ou l'****interconnexion****, ainsi que le* ***verrouillage****, l'****effacement*** *ou la* ***destruction****.[. . .]*

Fichier de données à caractère personnel

Article 2

[. . .]Constitue un ***fichier de données à caractère personnel*** *tout* ***ensemble structuré et stable de données à caractère personnel*** *accessibles selon des critères déterminés.*

Traitement des fichiers automatisés ou non

Article 2

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel [...] à ***l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles****[...]*

Responsable de traitement

Article 3

Le responsable d'un traitement de données à caractère personnel est, [...] ***la personne [...] ou l'organisme qui détermine ses finalités et ses moyens***.

Traitement loyal et licite des données

Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1. *Les données sont collectées et traitées de **manière loyale et licite***
2. *Elles sont collectées pour des **finalités déterminées, explicites et légitimes***[a]

a. *Un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données*

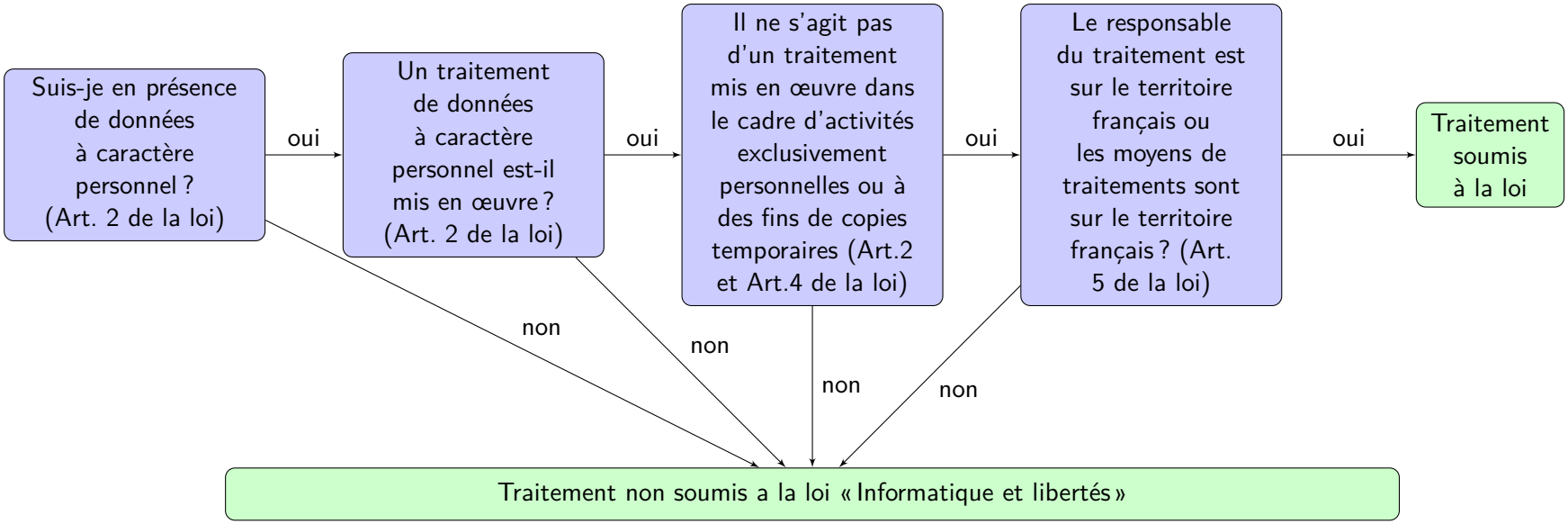
Traitement loyal et licite des données

Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

3. *Elles sont **adéquates**, **pertinentes** et **non excessives** au regard des finalités.*
4. *Elles sont **exactes**, **complètes** et, si nécessaire, **mises à jour**.*
5. *Elles sont conservées pendant une durée n'excédant pas **la durée nécessaire** au regard des finalités.*

Cas d'application de la loi Informatique et Libertés



Obligations incombant aux responsables de traitements

1. Obligation d'information lors du recueil des données (article 32) **y compris dans le cas de la collecte indirecte (article 32-3)** :
   - de l'identité du responsable du traitement,
   - de la finalité poursuivie par le traitement auquel les données sont destinées,
   - du caractère obligatoire ou facultatif des réponses,
   - des conséquences éventuelles, à son égard, d'un défaut de réponse,

Obligations incombant aux responsables de traitements

1. Obligation d'information lors du recueil des données (article 32) **y compris dans le cas de la collecte indirecte (article 32-3)** :
   - des destinataires ou catégories de destinataires des données,
   - des droits que la personne détient,
   - le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne,
   - dans le cas d'un service de communication électronique, l'abonné ou l'utilisateur doit être informé des moyens dont il dispose pour s'opposer ;

Obligations incombant aux responsables de traitements

2. Obligation d'assurer la sécurité des données (article 34) :
   - empêcher que les données soient déformées, endommagées,
   - ou que des tiers non autorisés y aient accès ;
3. Obligation d'informer l'intéressé en cas de violation de données à caractère personnel (uniquement les fournisseurs de services de communications électroniques accessibles au public - article 34 bis).

Obligations incombant aux responsables de traitements

3. Obligation de s'assurer qu'un sous-traitant présente des garanties suffisantes pour traiter des données à caractère personnel (article 35) :
   - obligations contractuelles,
   - ne décharge pas le responsable du traitement de son obligation de veiller au respect des mesures de sécurité,
   - cas particulier des hébergeur de données de santé (co-responsabilité des traitements) ;

Obligations incombant aux responsables de traitements

4. Obligation de fixer une durée de conservation des données (article 6°1)
   - sauf dans le cas de données appelées à être traitées à des fins historiques, statistiques ou scientifiques.
5. Interdiction de détournement de finalité (article 6°3)

Droits des personnes à l'égard des traitements de données à caractère personnel

1. Droit à l'information préalable (article 32 pour la collecte de données)
2. Droit d'accès : droit de demander à tout responsable de traitement s'il détient des informations l'intéressé (article 39)
   - le droit d'accès direct,
   - le droit d'accès indirect ;

Droits des personnes à l'égard des traitements de données à caractère personnel

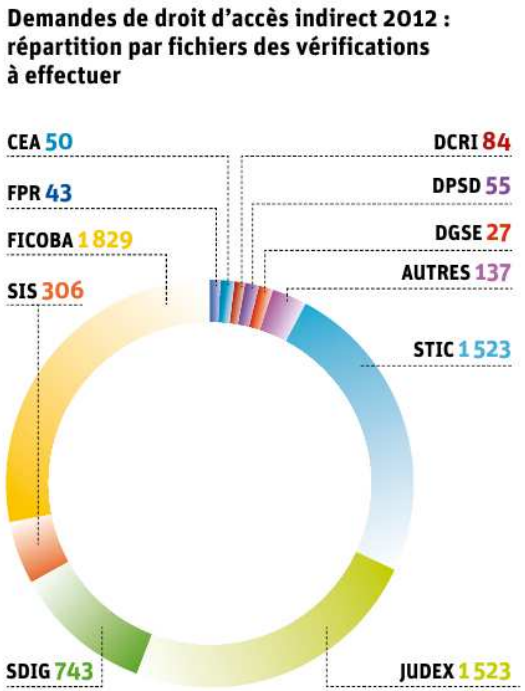
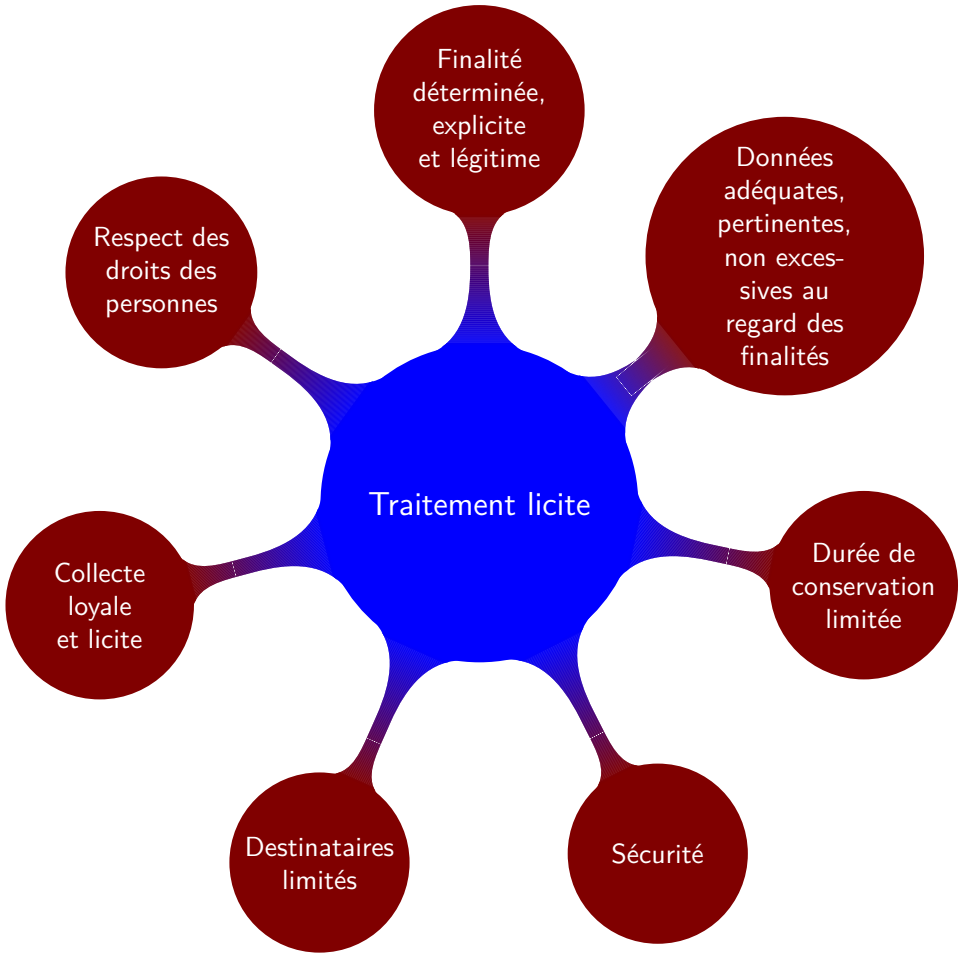


FIGURE : Extrait du rapport annuel 2012 de la CNIL

Droits des personnes à l'égard des traitements de données à caractère personnel

3. le droit de rectification
4. Droit d'opposition pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (article 38) ;
   - Droit d'opposition sans motivation à la prospection (article 38)

Traitement licite de données à caractère personnel



Formalités préalables

Depuis 2004 :

- Allègement du contrôle *a priori* (formalités préalables)
- Renforcement des contrôles *a posteriori* (pouvoir de sanction)

Formalités préalables (La déclaration normale)

Différents régimes de formalités préalables :

- La déclaration normale
- La formalité simplifiée associée (engagement de conformité)
  - Norme simplifiée (« NS »)

Quelques exemples de normes simplifiées :

- NS 42 : contrôle d'accès aux locaux, horaires, restauration sur le lieu de travail
- NS 46 : gestion du personnel
- NS 48 : fichiers de clients et de prospects

Formalités préalables (La demande d'autorisation)

2 critères justifient la nécessité d'effectuer une demande d'autorisation :

1. la finalité du traitement
   - permettre d'exclure du bénéfice d'un droit, d'une prestation ou d'un contrat
   - l'interconnexion de fichiers correspondant à des intérêts publics différents ou des finalités différentes [8]
   - Transfert hors UE (exceptions)
2. le traitement comporte les données suivantes :
   - données « sensibles » (Article 8 ou NIR)
   - données biométriques ou génétiques
   - données relatives aux infractions, condamnations et mesures de sûreté

8. C'est le cas de croisement de fichiers pour détecter de fraudeurs aux allocations

Formalités préalables (La demande d'autorisation)

Différents régimes de formalités préalables :

- La demande d'autorisation
- La formalité simplifiée (engagement de conformité)
  - Autorisation unique (« AU »)

Quelques exemples d'autorisations uniques :

- AU 17 : gestion du pré-contentieux et du contentieux pour les infractions constatées par les commerçants
- AU 19 : utilisation du réseau veineux pour l'accès à des locaux professionnels
- AU 27 : reconnaissance de l'empreinte digitale pour le contrôle de l'accès aux postes informatiques portables professionnels

Formalités préalables (La demande d'avis)

6 critères justifient la nécessité d'effectuer une demande d'avis :

- la sûreté, la défense ou la sécurité publique
- la prévention, la recherche, la constatation ou la poursuite d'infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté
- l'utilisation du NIR (numéro de sécurité sociale) ou la consultation du RNIPP (lorsque les organismes ne sont pas déjà habilités) ;
- l'utilisation de données biométriques [9]
- le recensement de la population ;
- les téléservices de l'administration électronique

9. empreintes digitales, contour de la main, iris de l'œil, etc.)

Formalités préalables (La demande d'avis)

Différents régimes de formalités préalables :

- La demande d'avis
- La formalité simplifiée (engagement de conformité)
  - Acte réglementaire unique (« RU »)

Quelques exemples d'actes réglementaires uniques :

- RU 20 : relatif aux procédures d'appel à témoins
- RU 31 : vidéoprotection au sein des locaux et des établissements de l'administration pénitentiaire
- RU 33 : relatif aux interdictions de paris sportifs

Le Correspondant Informatique et Libertés

- tout organisme peut désigner un CIL
- un vecteur de sécurité juridique
- une source de sécurité informatique
- soulagé du régime déclaratif
- obligation de tenir un registre des traitements
- obligation de faire un bilan de ses activités chaque année

Une nouvelle compétence

Distinction entre

- « vidéosurveillance » (application de la loi Informatique et Libertés)
- « vidéoprotection » (code de la sécurité intérieure [10])
- la CNIL dispose du pouvoir de contrôle des dispositifs de vidéoprotection [11]
- 173 contrôles vidéo pour l'année 2012

10. Code de la sécurité intérieure sur Legifrance

11. loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite LOPPSI 2)

Les plaintes

- dispositif de plainte en ligne
- intérêt marqué des personnes pour la protection de leurs données personnelles

Plaintes fréquentes :

- Surveillance permanente de salariés
- Droit d'accès
- Droit à l'oubli

Les contrôles

- stratégie issue directement de l'esprit de la loi (article 44)
- des compétences élargies (dispositifs vidéo)
- évolution significative (42 contrôles en 2004, 458 en 2012)
  - 285 contrôles en 2012 portant sur des dispositifs relevant de la loi Informatique et Liberté
  - 173 contrôles portant sur des dispositifs de vidéoprotection/vidéosurveillance

Les origines des contrôles

- 23% suite à l'instruction des plaintes
- 11% dans le cadre de procédure de sanction
- 26% au regard de l'actualité
- 40% inscrits dans les thématiques annuelles [12]

12.

- Programme annuel 2012 :
  - La sécurité des données de santé
  - les failles de sécurité
  - Sport et vie privée
  - les données à caractère personnel et la vie quotidienne
  - la délivrance des visas
- Programme annuel 2013 :
  - le traitement des données par les instituts de sondage
  - Les données traitées dans le cadre de l'internet en libre accès
  - Le traitement par les collectivités locales des données relatives aux difficultés sociales des personnes
  - Les données des personnes détenues en établissements pénitentiaires

Les différents types de contrôle

- Le contrôle sur place (article 44)
- Le contrôle sur pièces(article 44-III) :
- L'audition sur convocation (article 44-III)

Les principaux manquements constatés en contrôle

- absence de durée de conservation (article 6-5) ;
- défauts de sécurité (article 34) ;
- présence de données excessives (article 6-3) voire illégales (article 8) [13]
- défaut d'information des personnes (article 32) ;
- données d'infraction (article 9)

13. Danger des zones blocs-notes et commentaires

Les différentes sanctions prononcées par la formation restreinte

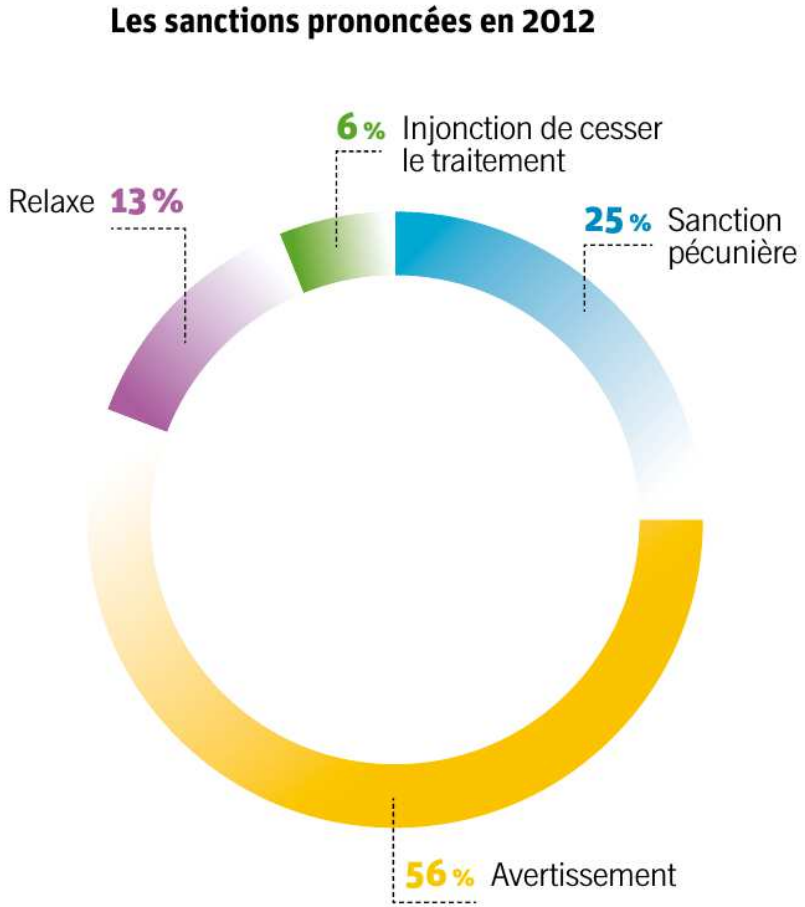


FIGURE : Extrait du rapport annuel 2012 de la CNIL

Les manquements proposés dans les rapports de sanction en 2012

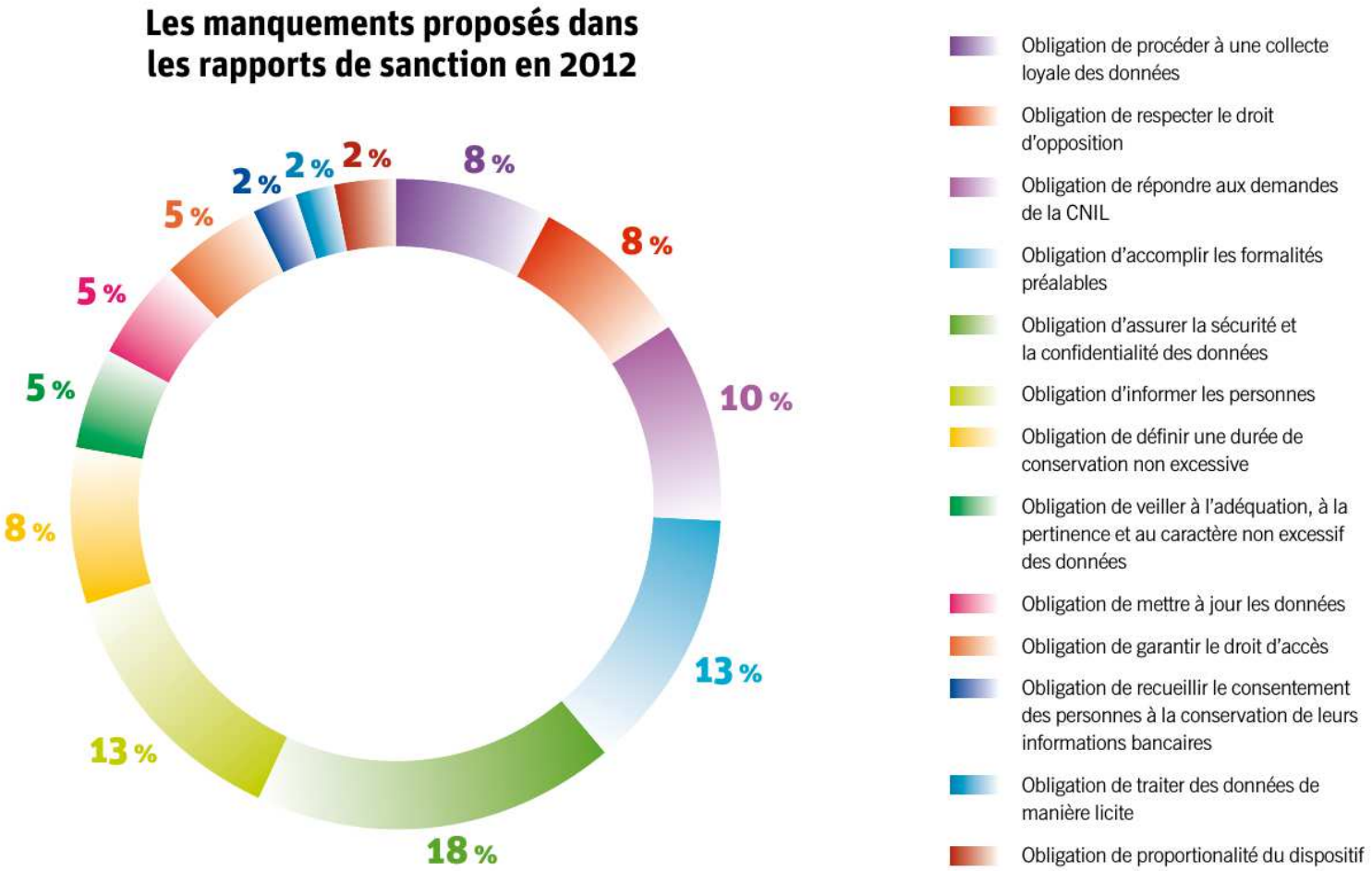


FIGURE : Extrait du rapport annuel 2012 de la CNIL

Table des matières

Destinataire et tiers autorisé

Article 3-2

Le destinataire d'un traitement de données à caractère personnel est ***toute personne habilitée à recevoir communication de ces données*** *autre que la personne concernée, [. . .]*

- Seuls les destinataires et les tiers autorisés peuvent avoir accès aux informations

Identification et authentification

- Identification : « je dis qui je suis »
- Authentification : « je prouve qui je suis »

- on identifie une personne, pas un groupe de personnes [14]

14. l'identification porte en général sur des personnes mais également sur des machines

L'authentification

- Par un secret que je connais
  - mot de passe
  - défi (question réponse)
- par quelque chose que je possède
  - certificats
  - carte à puce
- par ce que je suis
  - biométrie

L'authentification forte cumule les différents facteurs

Table des matières

Des données d'un nouveau genre

- Données ouvertes (*open data*)
- Myriades de données (*big data*)
- Auto-mesure de soi (*quantified self*)

Merci ☺

Des questions ?