

LES ASPECTS LEGAUX LIES A LA CONFIDENTIALITE, LA SECURITE & L'INTEGRITE DES DONNEES MEDICALES INFORMATISEES & A LA PROTECTION DES INDIVIDUS :

Présentation de la réglementation

**Aude BONNARD
2026**

« L'informatique doit être au service de chaque citoyen....elle ne doit pas porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques;

Tte personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi. »

Objectif de la réglementation

« Informatique doit être au service de chaque citoyen »



- ☒ Identité humaine
- ☒ Drts de l'Homme
- ☒ Vie privée
- ☒ Libertés individuelles ou pub.

Objectif de la réglementation

➤ Définir

➤ Encadrer



Protection de la vie privée contre le fichage

➤ Sanctionner



LE TEXTE EUROPEEN

☐ RGPD 27/04/2016

Définition

Objectif

Régulation

Marge de manœuvre des Etats (données génétiques, biométriques, données de santé)



LES TEXTES NATIONAUX

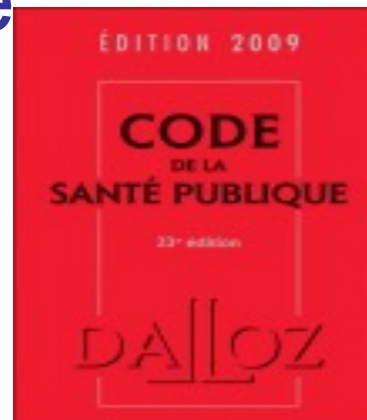
- **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
(« *Loi informatique et liberté* »)

Modifiée en 1994, 2004

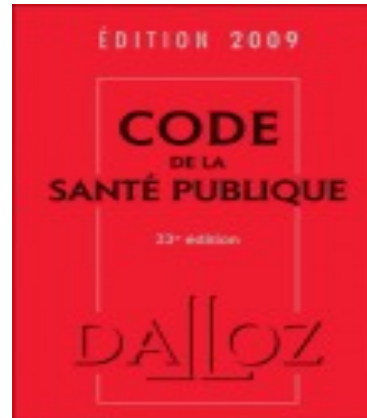
Loi 20/06/2018 protection des données personnelles

LES TEXTES NATIONAUX

- ❑ Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé



Art. L.1110-4



« Toute personne prise en charge par *un professionnel de santé, un établissement ou service (...)* a le droit au respect de sa vie privée et du secret des informations la concernant (...).



LA C.N.I.L

« autorité en charge de veiller à la protection des données personnelles. A ce titre, elle dispose notamment d'un pouvoir de contrôle et de sanction. Jouant aussi un rôle d'alerte et de conseil, elle a pour mission de veiller à ce que le développement des nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »

LA C.N.I.L

Son Statut

Autorité administrative indépendante
Définition

LA C.N.I.L

Sa Composition

18 membres



12 mbres élus par leurs pairs

- 2 députés

- 2 sénateurs

- 2 Conseil Eco & Social

- 2 Cour de Cassation

- 2 Conseil d'Etat

- 2 Cour des Comptes

LA C.N.I.L

Sa Composition



3 personnes compétentes en informatique



3 personnes désignées par décret pris en Conseil des Ministres

LA C.N.I.L

Son Rôle

**VEILLER A LA BONNE APPLICATION DE LA
LOI INFORMATIQUE & LIBERTE**



2 Pouvoirs

Pouvoir de conseil

Pouvoir de contrôle : investigation
mise en garde
sanction (2004)

Explications et illustrations

Illustrations

CE 12 Juillet 2024

CNIL est libre :

- dans son appréciation des faits
- Dans le choix des sanctions



09/01/2018 100.000€

Données des clients ayant effectués 1
demande en ligne au service après vente

=

Insuffisamment sécurisées



Janvier 2019

Amende 50 millions €

=

Défaut d'info des utilisateurs sur
l'exploitation des données



Décision 07/12/2020

Amende de 3.000€ et 6.000€

Sur serveur de 2 médecins images médicales en libre accès
sur internet

=

Manquement à leur O de sécurité

DOMAINE DE LA LOI

Définir

=

Qd la loi s'applique ?

RGPD

*"toute opération ou tt ensemble d'opération effectuées ou non à l'aide de **procédés automatisés** et appliqués à des données ou ensemble de **données caractère personnel**, collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, modification, diffusion, rapprochement, interconnexion, limitation, effacement ou destruction"*

La Loi

« *La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles (...)* » Art 2

Définition extensive

→ traitement

→ données à caractère personnel

Traitement automatisé



Traitement non automatisé



Examples



fichier papier

=

Ensemble structuré et stable de données à
caractère personnel

Traitement automatisé (fichier informatique, clef USB...) ou non (fichier papier, manuel) contenant des **info. relatives à des personnes physiques**, destinées à usage non personnel

=

Données à caractère personnel

Définition des données personnelles

❖ RGDP

« *Tte info se rapportant à une PP **identifiée** ou **identifiable*** »

Définition des données personnelles

❖ **Loi = + précise**

« Tte info relative à une PP identifiée ou qui peut-être **identifiée directement** ou **indirectement**, par référence à un n° d'identification ou à plusieurs éléments qui lui sont propres ».

données de santé
=
données à caractère personnel
=
données sensibles

(Génétiques,Biométries,Orientation sexuelle des personnes)

=
Protection

Déf. Données de santé-RGPD

« Données relatives à la santé physique ou mentale, passée, présente, future, d'une PP (y compris la prestation de services de soins de santé) qui révèlent des info sur l'état de santé de cette personne ».

Données de santé-CNIL

Déf. + large

« Toute donnée relative à la santé d'une personne ou susceptible de donner une indication sur son état de santé »

Illustrations

① Données de santé par nature

maladies, antécédents, traitements, handicap...

② Données par croisement avec d'autres données deviennent données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne (poids-apports caloriques)

③ Données en raison de leur destination, utilisation

Données de santé



Directement nominatives
Indirectement nominatives

Info directement nominative

➔ Dossier médical (identité du patient)

➔ Traitement qui ne comporte pas le nom du patient mais l'enregistre sous un n° ou un code renvoyant à une table de correspondance (papier ou informatique)

Indirectement nominatives

Illustrations

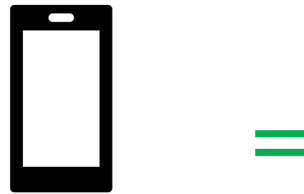
CNIL 5 sept 2024

Condamnation
logiciel médical



Données indirectement identifiables

Ne sont pas des données de santé :
données à usage exclusif de la personne



Applications mobiles sur smartphone ou
tablette sans connexion extérieure et à
usage personnel

Exemples de données « borderline »

RGDP n'oublie t-il pas les données frontières
?

Données personnelles non médicales
collectées par le prof de santé au cours d'un
examen

=

Vie personnelle, prof., élt sociaux...

SECRET PROFESSIONNEL



Les O du responsable du fichier

RGPD= Allégement des formalités



Ppe d'accountability

Les O du Prof de santé

- ☒ Mise en place registre de traitement
- ☐ Faire des analyses d'impact (logiciel)
- ☒ Informer les personnes concernées
- ☐ Formaliser les rôles et responsabilités du responsable
- ☐ Désigner un DPD

4 obligations légales

- ▶ Obligation de respecter la finalité des données
- ▶ Obligation de sécurité
- ▶ Obligation de confidentialité
- ▶ Obligation de respecter la durée de conservation des données

RESPECTER LA FINALITE

Dossier papier
Logiciel médico-ad

=

Finalité
déterminée
explicite
légitime

Respecter la finalité

Données collectées nécessaires aux activités de :

- ☐ soins,
- ☐ prévention,
- ☐ diagnostic,
- ☐ gestion du cabinet



Adéquates



Pertinentes



Limitée à ce qui est nécessaire à la prise en charge du patient

Illustrations

O. Respecter la finalité

Une Exception

La notion « d'extension de finalité »

La CNIL admet que des traitements puissent être utilisés à des fins autres que celles prévues à l'origine dans la mesure où l'utilisation secondaire se situe dans le prolongement de l'utilisation du fichier de base.

Notion utilisée en matière de **recherche médicale** : La CNIL se fonde sur cette notion p/o autoriser, dans certaines conditions, l'accès des chercheurs à des fichiers de gestion afin de servir de base à des études épidémiologiques.

Obligation de sécurité

Qui :

- *toute personne collectant, ordonnant ou effectuant un traitement de données médicales*
- *intervenant dans le traitement ou la conservation des données*

Pourquoi
Déformées,
Endommagées
Communiquées à des tiers non autorisés .

Pour le dossier médical :

- ⇒ Mot de passe individuel (renouvelé)
- ⇒ antivirus, parfeu,
- ⇒ sauvegarde, conservation sur 12 mois glissant
- ⇒ Chiffrement des données
- ⇒ verrouillage au-delà d'1 courte période de pose
- ⇒ absence ou minimisation connexion appareils non professionnels

Pour les échanges de données via Internet

- ⇒ cryptage des info
- ⇒ mise en place de procédures d'authentification d'identification individuelle et mise en œuvre de dispositif de filtrage des accès (firewall)

transfert à distance d'imagerie médicale via réseau numéris

- ☐ Cryptage des données d'identification des patients avant transmission des données;
- ☐ Les utilisateurs doivent être nommément habilités et disposer d'un code d'utilisateur personnel et d'un mot de passe;
- ☐ Tenue d'un journal des connexions;
- ☐ Mise en place d'un système assurant la détection de toutes les erreurs de transmission.

- « **Messagerie Sécurisée de Santé** » :
mis en œuvre par l'ASIP Santé-
messagerie sécurisé permet échange info
entre prof de santé participant à la prise
en charge d'un même patient.

Illustrations

O. de Confidentialité

- Notion voisine de l'O. de sécurité :
Sécurité = Confidentialité
- O. impérative pour la CNIL
- Le prof, le personnel(engagement de confidentialité)

Illustrations

Anonymisation

Réversible



Table de concordance

=

Ré-identification

Irréversible

=

préconisée dans la
surveillance obligatoire
des maladies
infectieuses

O. Respecter une Durée

=

Principe Droit à l'oubli

Les données ne doivent pas être conservées sauf accord de la CNIL, au-delà de la durée nécessaire aux finalités du traitement pour lesquelles elles ont été enregistrées.

Durée de conservation des dossiers médicaux

Exceptions

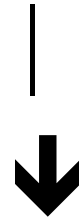
Durée de conservation des dossiers médicaux

- Cabinets médicaux ► ?



Suspension du délai

- 1^{ère} Exception : Action en Resp.médicale



Fin de l'action

- 2 Exception : La minorité



Suspension jusqu'à la majorité du patient

3ième exception patient dcd moins de
10 ans après dernière consultation



10 ans à compter de la date du dc

Doubles des feuilles de soins



3 mois

Surveillance épidémiologique et recherche sur le Covid 19 (D 07/08/2020)



- 6 mois à compter de la fin de l'état d'urgence

LA RECHERCHE MEDICALE

(Loi 26/01/2016 – Ord 16/06/2016)

Impliquant la personne humaine

=

- Recherche interventionnelle non justifiée par prise en charge habituelle
- Recherche interventionnelle avec risque et contraintes minimales
- Recherche non interventionnelle

Un principe

Intérêt de la personne doit primer sur les
intérêts de la science et de la société

Sujet de la recherche

- ☐ Personne en vie
- ☐ Personne dcd-consentement du vivant ou témoignage de la famille
- ☐ Embryon (loi 06/08/2004)
- ☐ Mineur avec autorisation d'un parent
- ☒ ~~Mesure de sauvegarde de justice~~

Recherche impliquant la personne humaine

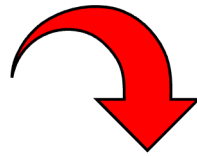
=

Formalisme

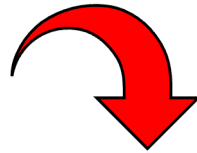
Contrôle

Ppe du contrôle préalable

Promoteur d'un projet de recherche



Avis du CPP



Autorisation préalable de la CNIL

CPP



CPP avis obligatoire

Caractère décisionnel de l'avis du CPP

- 45 j pour donner son avis
- Silence = rejet
- Si dans les 2 ans qui suivent l'avis la recherche n'a pas débutée=avis caduc
- Recours pour excès de pouvoir

Autorisation préalable de la CNIL

Pour les traitements de données
personnelles ayant une finalité :

- D'intérêt public de recherche médicale
- D'étude ou d'évaluation dans le domaine médical



Dépôt d'un dossier complet auprès de la CNIL

- ① L'avis du CPP
- ② Le détail des mesures relatives à l'info des personnes se prêtant à la recherche
- ③ L'identité et l'adresse du responsable du traitement ;
- ④ La ou les finalités du traitement, s'il y a lieu, la dénomination du traitement ;
- ⑤ Le ou les services chargés de la mise en oeuvre du traitement ;

- ⑥ Le service auprès duquel s'exerce le droit d'accès des participants et les mesures prises pour faciliter l'exercice de ce droit ;
- ⑦ Les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
- ⑧ Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
- ⑨ Le cas échéant, les interconnexions, les rapprochements ou toute autre forme de mise en relation avec d'autres traitements.



La CNIL dispose d'un délai de 2 mois, renouvelable une fois, autoriser le projet.

Si à l'expiration de ces 2 mois, elle ne s'est pas prononcée = autorisation refusée

Durée de conservation : recherche biomédicale

- ⇒ 12 mois « *après la fin de la dernière recherche à laquelle a participé la personne* »
- ⇒ 15 ans au maximum si données anonymisées de manière irréversible ou conservées à des fins statistiques, historiques ou scientifiques

DROITS DES PERSONNES FICHEES

Ce sont des droits généraux

=

Tous les fichiers (informatisés et manuels,
mécanographiques)

Droit de Contrôle

DROITS DE CONTRÔLE A PRIORI

① Droit d'Être Informé (transparence)

🗣️ Droit d'Opposition

Droit d'être informé

Information = consentement
Confiance

Non info. du patient

Info délétère = droit de se taire



Intérêt de la santé du patient



recherche médicale

=

Droit renforcé

Information renforcée

=

Les participants doivent être informés
individuellement et par écrit

Droit d'opposition

Le dt d'information est complété par la reconnaissance d'un **dt de s'opposer** à ce que les données personnelles fassent l'objet d'un traitement

Droit d'opposition relatif

Nécessite de l'existence de « *raisons légitimes* » invoquées par le patient

▪

Exemple de motifs légitimes

Avis favorable de la CNIL

« Le droit d'opposition prévue par la loi ne s'applique pas lorsque le traitement répond à une obligation légale

Dt d'opposition renforcé en matière de recherche médicale

Le patient n' a pas à motiver son refus au
traitement informatique de données le
concernant

Droit de Contrôle a posteriori

Droit d'Accès

Droit de Rectification, effacement

Droit d'Accès

Conditions Droit d'Accès

Non respect du délai

Illustration : Condamnation d'un chirurgien dentiste

Droit de Rectification

(sans frais po demandeur)

Droit pour le patient « *d'exiger que soit rectifiées, complétées, clarifiées, mises à jour ou effacées, les informations qui sont inexactes, incomplète, équivoques, périmées ou dont l'utilisation, la communication ou la conservation est interdite* ».

Recommandations de la CNIL en cas d'effacement d'une donnée

- ❑ Conservation de la mention de la suppression = Traçabilité
- ❑ Effacement d'une donnée n'interdit pas son archivage par le médecin sur un support papier ou un support physique amovible, de type CD non réinscriptible.

LES SANCTIONS

☹ Article 226-16 à 226-24 Code Pénal

Sanctions pénales

=



5 ans d'emprisonnement

+



300.000 Euros d'amende

☹ Code Pénal (L.06/08/2004)

«Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans mettre en œuvre les mesures prescrites par la Loi est puni... »

LA CNIL

La Procédure

- ➔ Connaissance d'un manquement à la Loi
- ➔ Formation contentieuse de la CNIL
- ➔ Elle peut prononcer :
 - ❶ Avertissement avec publicité
 - ❷ Mise en demeure du resp. (10 j → 3 mois)

Mise en
demeure



**Mise en
conformité**



**Dossier
classé**

Sans effet



**Audition du resp.
Procédure
contradictoire**



Sanctions

LA C.N.I.L

Sanctions pécuniaires

- **1^{er} Manquement**
 $\leq 150.000\text{€}$
- **Manquement réitéré ds les 5 ans**
 $\leq 300.000\text{€}$

Emprisonnement

5 ans

Sanctions PM

- Amende = 1 000 000€
- Interdiction d'exercer à titre définitif ou pour 5 ans
- Fermeture déf ou pour 5ans
- Exclusion des marchés pub. déf ou 5 ans
- Interdiction po 5 ans ou + d'émettre des chèques ou usage CB

Examples



1

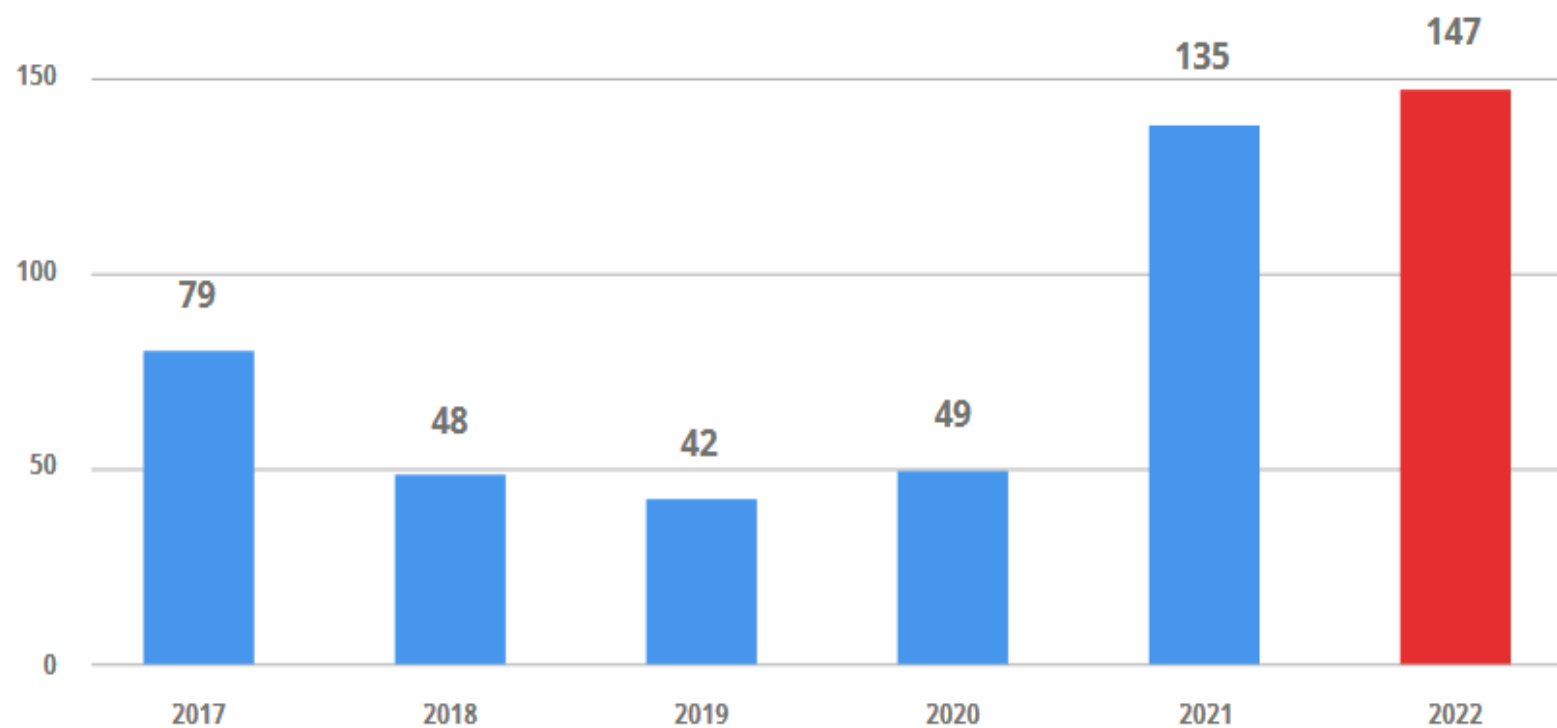
sur 1



Zoom automatique



Mises en demeure de la CNIL 2022



500
millions d'euros
d'amendes

prononcées pour des manquements
au RGPD, à la loi Informatique et
Liberté ou à la directive ePrivacy.

Parmi ces sanctions

Amazon

35 M€ en 2020

Microsoft

60 M€ en 2022

Google

50 M€ en 2019

100 M€ en 2020

150 M€ en 2021

Facebook

60 M€ en 2021

Apple

8 M€ en 2022

Autorités européennes de protection des données

2,5
milliards d'euros
d'amendes

prononcées par les autorités européennes
de protection des données pour des
manquements au RGPD

Free mobile=300.000€

04/01/2022

Droits des personnes et sécurité des données

Sanction de 300 000 euros à l'encontre de FREE MOBILE



LES INVESTIGATIONS

Plusieurs plaintes ont été adressées à la CNIL contre FREE MOBILE, qui ne permettait pas aux personnes :

- **d'accéder aux données les concernant ;**
- **de s'opposer à la réception de messages de prospection.**



LES MANQUEMENTS

- Manquements aux droits des personnes concernées (**droit d'accès et droit d'opposition**) ;
- **Défaut de protection des données dès la conception** (processus produisant des informations obsolètes) ;
- Défaut de **sécurité des données** (transmission de mots de passe non temporaires en clair par courriel).



LA DÉCISION

La formation restreinte de la CNIL a prononcé une sanction de 300 000 euros à l'encontre de la société FREE MOBILE.

Google=150millions€
Facebook= 60 millions €

06/01/2022

Refuser les cookies doit être aussi simple qu'accepter

La CNIL sanctionne GOOGLE et FACEBOOK



LES INVESTIGATIONS

La CNIL a reçu plusieurs plaintes dénonçant les modalités de **refus des cookies** sur les sites web **facebook.com, google.fr** et **youtube.com**.

Des contrôles en ligne ont été effectués sur ces sites.



LES MANQUEMENTS

Un bouton permet d'accepter immédiatement les cookies mais **il n'existe pas de solution équivalente pour les refuser aussi facilement.**

Ce procédé porte **atteinte à la liberté du consentement** des internautes et constitue une **violation de l'article 82 de la loi Informatique et Libertés.**



LA DÉCISION

La formation restreinte de la CNIL a prononcé :

- une amende de 60 millions d'euros à l'encontre FACEBOOK ;

- deux amendes pour un montant total de 150 millions d'euros à l'encontre de GOOGLE.

RATP de 400 000 €

04 novembre 2021

- Collecte de données non nécessaires
- Manquement à O de sécurité
- Manquement à O de limiter la durée de conservation des données

Doctissimo-Cnil 11/05/2023

- Plaignant =Privacy International (Ass. GB)
- Amende = 380.000€
- Manquement à l'O de recueillir consentement des personnes
- Non sécurité de la navigation du site
- Cookies publicitaires
- Gestion des mots de passe insuffisante

Plaintes-Secteurs d'Activité

