Protection de la vie privée et des données à caractère personnel

Guillaume Piolle
guillaume.piolle@centralesupelec.fr
http://guillaume.piolle.fr/

CentraleSupélec, campus de Rennes

5 décembre 2016

Ce qui est privé est-il honteux ?

Si vous n'avez rien à vous reprocher, alors vous n'avez rien à cacher.

- Mais alors, pourquoi utiliser une enveloppe lorsque vous envoyez une lettre ?
- Ce n'est pas parce que vous n'avez « rien à cacher » que rien ne pourra vous être reproché ou que rien ne pourra vous blesser.

Ce genre de déclaration est habituellement faite par un membre d'une « caste dominante » : un homme, blanc, hétérosexuel, si possible de plus de 45 ans.

Les risques : la brèche de vie privée

Formes principales

- Intrusion d'une personne dans vos affaires « privées » ;
- Révélation au public ou à un tiers d'une information « privée » que vous n'étiez pas prêt(e) à divulguer, et/ou qui est fausse ;
- Vol d'identité.

Conséquences possibles

- Impact (plus ou moins grave) sur les relations sociales ;
- Risque de discrimination ;
- Risque de poursuites pénales ;
- ...

Et les personnes « publiques » ?

Les risques : Le vol d'identité

Symptômes (`identitytheft.org.uk`)

- Perte de papiers d'identité ;
- Les courriers (banque notamment) ne vous parviennent plus ;
- Opérations bancaires inhabituelles ;
- On vous informe que vous avez fait une demande de prêt, d'aide sociale ou gouvernementale ;
- Vous recevez des factures, injonctions de payer ou mises en demeures pour des biens ou services dont vous n'avez pas connaissance ;
- On vous refuse un crédit alors que vous avez un bon dossier ;
- Un contrat de téléphonie mobile a été souscrit en votre nom ;
- Vous êtes contactés par des organismes bancaires avec lesquels vous n'avez pas de contacts habituellement ;
- ...

Quel rapport avec l'informatique ?

La notion de vie privée, de droit à la vie privée, de protection de la vie privée. . . peut être considérée indépendamment de l'informatique

L'informatique (et Internet) apporte de **nouvelles sources de risques** mais également de **nouveaux outils de protection**.

Services web, *Cloud computing* et vie privée : Mat Honan

L'affaire Mat Honan

Journaliste *senior* du magazine *Wired*.

En août 2012, la totalité de ses comptes en ligne sont compromis et une grande partie de ses données sont détruites par quelques attaquants.

Les dégâts

- Compte Google compromis puis supprimé ;
- Compte Twitter compromis et utilisé pour diffuser des propos racistes et homophobes ;
- Compte Amazon compromis ;
- Compte AppleID compromis, permettant la suppression à distance de données sur ses iPhone, iPad et MacBook (une année de photos, 8 ans de messagerie Gmail).

Services web, *Cloud computing* et vie privée : Mat Honan

La motivation du hacker ?

Le contrôle de son compte Twitter, `@mat`, convoité car en trois caractères. . .

Les causes du désastre

- Liens systématiques entre les différentes identités ;
- Pas d'authentification à deux facteurs ;
- Pas de stratégie de sauvegarde efficace ;
- Applications Apple conçues pour contrôler les données de l'utilisateur depuis un service central (design « agressif » pour la vie privée) ;
- Failles critiques dans les procédures de sécurité d'Amazon et Apple (un numéro de carte de crédit partiel affiché par Amazon et utilisé comme facteur d'authentification par Apple).

Services web, *Cloud computing* et vie privée : Mat Honan

Ce qui a pu être récupéré

Reprise de contrôle des comptes en ligne, restauration de la plupart des données *cloud* (Gmail et compagnie), effacement du MacBook interrompu, essentiel des données récupéré.

Chez Mat Honan

Mise en place d'une réelle stratégie de sauvegarde, systématisation de l'authentification à double facteur, désactivation des services *Find my* d'Apple.

Réactions d'Amazon et Apple

- Amazon : correction de la faille organisationnelle ;
- Apple : engagement à revoir les procédures, mais les vulnérabilités sont restés exploitable pendant un moment.

Définitions générales et non techniques

La Sphère privée (Crépin 2008)

Ensemble des informations qu'une personne considère comme privées.

La spère privée est **personnelle**, **personnalisable** et **dépendante du contexte**.

Protection de la vie privée

Ensemble des mesures destinées à préserver le **contrôle** qu'une personne peut avoir sur sa sphère privée (périmètre et contenu).

La vie privée : une notion liée à la culture

En France

Droit fondamental, et même « fondamental fondamental », condition nécessaire à l'exercice des autres droits fondamentaux.
Dans le bloc constitutionnel depuis 1971.
Rôle central de l'État comme garant de ce droit.

Aux États-Unis

Ne peut entrer en conflit avec la liberté d'expression, juridiquement supérieure (premier amendement).
Défiance envers l'État.
Rôle central du marché, de la libre entreprise.

Historique

- Warren & Brandeis 1890 : *The Right to Privacy*. Premières réflexions suite aux progrès de la photographie ;
- Création progressive d'un droit à la vie privée dans la doctrine juridique, sous la forme d'un **droit de propriété incorporelle** lié aux **droits de la personne** ;
- 1970 : introduction du droit à la vie privée dans le Code civil français ;
- Fin des années 1970 : Scandale du fichier Safari, loi Informatique et Libertés ;
- Années 1990 et à suivre : trop denses pour être résumées ici !

Historique

Rappel :

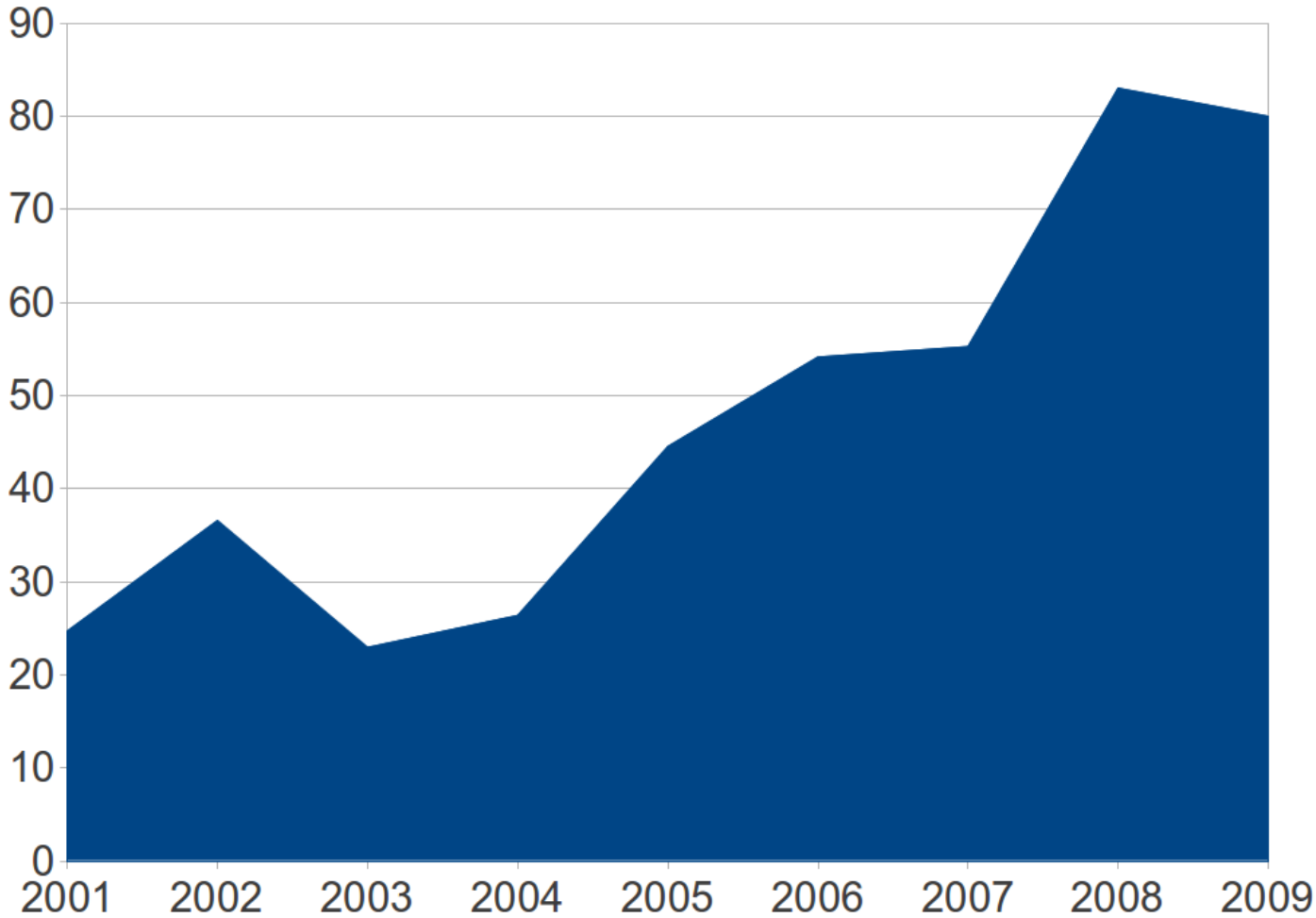
Historiquement, « l'ennemi » n'est pas Google ni Facebook, c'est l'État !

Depuis les années 2000, les inquiétudes liées à la vie privée se tournent vers d'autres acteurs.

Est-ce parce qu'il n'est plus nécessaire de se méfier de l'État ?

- Le fichier Safari a été réintroduit (Edvirsp dans la loi Loppsi 2, et il a de nombreux petits camarades (44 nouveaux entre 2002 et 2009) ;
- Nombreux fichiers illégaux à l'Intérieur et à la Défense (même à l'issue de la période de grâce après 2004) ;
- 2016 : Controverse autour du fichier des Titres Électroniques de Sécurité (TES), introduit par voie réglementaire ;
- Accès abusifs aux fichiers ;
- ...

Historique



Taux d'erreurs du fichier STIC (source : J.-M. Manach)

Droit à la vie privée *vs* Protection des données personnelles

Droit à la vie privée

Droit « correctif »
Notion de préjudice et de réparation
Il faut démontrer le préjudice

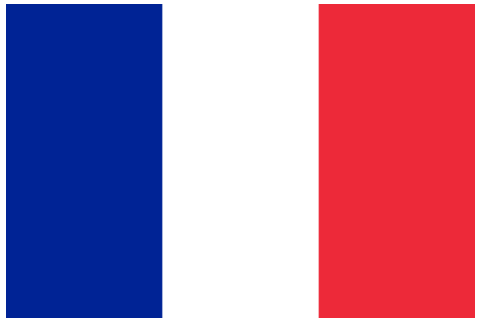
Protection des données personnelles

Droit « préventif »
Règles visant à éviter les violations de la vie privée
La violation des règles constitue un préjudice en soi, par principe

Contexte international

- **ONU :**
  - 1948 - Déclaration universelle des droits de l'homme (art. 12) ;
  - 1966-1980 : Pactes à force contraignante (droits civils et politiques, droits économiques, sociaux et culturels).
- **Conseil de l'Europe :**
  - 1950 - Convention de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8) ;
  - 1981 - **Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** (en particulier préambule, art. 5).
- **Union européenne :**
  - 1992-2007 - Traité de l'Union européenne (inclut la CSDHLF) ;
  - 2000-2010 - Charte des droits fondamentaux de l'Union européenne ;
  - 1995 : **Directive 95/46/CE**
  - 2002 : Directive 2002/58/CE
  - 2016 : **Réglement Général sur la Protection des Données** (RGDP/GDPR, en vigueur en 2018).

Contexte national en France



- **Code civil**, article 9 ;
- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés ;
- **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 ;
- **Loi n° 2016-1321 du 7 octobre 2016** pour une République numérique.

`http://www.legifrance.gouv.fr/`

Périmètre

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**.

Périmètre

Article 2 (extrait)

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, lorsque leur responsable remplit les conditions prévues à l'article 5.

Périmètre

Donnée à caractère personnel (donnée personnelle)

Suite de l'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. 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**.

Avant 2004 (cf directive 95/46), on parle d'*informations nominatives* ou *indirectement nominatives*.

Acteurs

Les acteurs décrits par la loi

- Le responsable de traitement ;
- La personne concernée (sujet des données) ;
- Les destinataires ;
- Les sous-traitants ;
- La CNIL ;
- Le CIL.

Principe de légalité

Données sensibles (art. 8)

Il est interdit de procéder à des traitements portant sur des données sensibles :

- Origines raciales ou ethniques ;
- Opinions politiques, philosophiques, religieuses ;
- Appartenance syndicale ;
- Santé et vie sexuelle.

Exceptions : consentement exprès, sauvegarde de la vie humaine, gestion des listes de membres, données déjà rendues publiques par la personne concernée, services de santé, statistiques officielles, recherche médicale, « intérêt public » (strictement encadré).

Principe de finalité

Art. 6, 2°

On collecte des données personnelles en vue d'une **finalité** déterminée (et pas « au cas où »).

On ne peut pas utiliser les données de manière incompatible avec la finalité initialement prévue.

Principe de légitimité

Art. 6, 2°

La finalité déclarée doit être **légitime**.

Voir le rôle du responsable de traitement vis-à-vis de la personne concernée : est-ce une finalité légitime pour une société de transports en commun de mettre en place des traitements de données visant à la gestion d'une régie publicitaire ?

cf. notion d'**intérêt légitime** comme fondement au traitement.

Principe de proportionnalité

Art. 6, 3°

La collecte doit être **proportionnée** (nature et quantité des données) à la finalité.

Données « adéquates, pertinentes et non excessives », + objectives et licites.

Adéquation de la durée de conservation (5°)

Pour des contre-exemples, voir 95 % des formulaires d'inscription sur Internet...

Formalités préalables

Les différents régimes

- **Déclaration (normale ou simplifiée, à la CNIL ou au CIL) :** cas général ;
- **Dispense de déclaration :** certains traitements particuliers (« sans risques ») visés par la CNIL ou par la loi ;
- **Autorisation ou avis :** traitements portant sur certaines catégories de données : données sensibles, génétiques, biométriques, relatives aux infractions ou condamnations, susceptibles de priver d'un droit, utilisant le numéro INSEE...

Droits des personnes concernées

- Droit d'être informé (art. 32) ;
- Droit d'opposition *pour motif légitime* (art. 38) ;
- Droit d'accès (art. 39) ;
- Droit de rectification, de suppression *en cas de non-conformité* ou si la personne est mineure (art. 40).

Mentions obligatoires

À faire figurer lors de la collecte :

- Droits des personnes ;
- Identité du responsable de traitement ;
- Finalité du traitement ;
- Destinataire des données ;
- Existence de flux transfrontaliers ;
- (Pour un questionnaire) caractère obligatoire ou facultatif des réponses ;
- (Pour un questionnaire) conséquences d'un défaut de réponse.

Sécurité et conservation des données

Obligation de sécurité

Les données appartiennent toujours à la personne concernée (encore que...), mais le responsable de traitement a une obligation d'assurer « la sécurité des traitements et des données » et d'empêcher qu'elles soient « déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Destruction des données

À la fin de la période de conservation et sauf exceptions, le responsable du traitement doit **détruire** les données, ou les « anonymiser » (illusoire, voir intervention suivante).

Commission Nationale de l'Informatique et des Libertés

Première autorité administrative indépendante en France (même statut que la Hadopi, par exemple).

Créée par la loi de 78, compétences modifiées par les lois de 2004 et 2016.

Membre français du G29.

Mission d'**information** et de **contrôle**.

`http://www.cnil.fr/`, nombreuses ressources en ligne (mais de moins en moins accessibles depuis la refonte de leur site web. . .)

Encadrement des formalités préalables

La CNIL. . .

- Est destinataire des déclarations normales et simplifiées ;
- Délivre les autorisations pour les traitements portant sur des données sensibles ;
- Émet des avis sur les traitements mis en œuvre par arrêté ministériel, par décret en Conseil d'État ou par certains organismes en situation de service public ;
- Répond aux demandes d'accès indirect ;
- Peut délivrer des « labels ».

La CNIL doit être consultée sur tout projet de loi ou de décret concernant son périmètre juridique et peut faire des propositions législatives ou réglementaires.

Mission de contrôle-sanction

La CNIL. . .

- Organise des contrôles spontanés auprès des responsables de traitements ;
- Reçoit les « réclamations, pétitions et plaintes » et éventuellement y donne suite ;
- En cas de saisine ou de constatation d'une infraction, la CNIL peut :
  - Classer sans suite ;
  - Organiser une médiation ;
  - Procéder à un contrôle ;
  - Émettre un avertissement, une mise en demeure, une injonction de cesser le traitement, un retrait d'autorisation ;
  - Infliger elle-même une sanction (~~jusqu'à 150 000 €, puis 300 000 € plafonnés à 5 % du CA en cas de récidive~~ porté à 3 000 000 € en 2016).

La CNIL doit informer le procureur de la République des infractions dont elle a connaissance.

Statistiques sur l'activité de contrôle-sanction

Exemple : le rapport d'activité 2009

- Évolution constante du nombre de contrôles (de 96 en 2005 à 270 en 2009) ;
- Principaux manquements constatés en contrôle :
  - Collecte déloyale (27 %) ;
  - Pertinence et mise à jour des données (23 %) ;
  - Information, droit d'accès ou d'opposition (19 %) ;
  - Communication à des tiers non autorisés (6 %) ;
  - Sécurité et confidentialité des données (6 %) ;
  - Défaut de consentement préalable (5 %).

Critique de la CNIL

Rendue « inoffensive » pour l'État

Depuis la loi de 2004, la CNIL n'a plus de pouvoir de contrôle sur l'État. Elle ne fait qu'émettre un **avis**, qui n'est pas nécessairement suivi (il faut alors un décret en Conseil d'État. . . mais l'avis du CE n'est pas nécessairement suivi non plus par le gouvernement).

Une autorité de contrôle trop complaisante ?

Sanctions souvent jugées beaucoup trop faibles en regard des infractions (beaucoup d'avertissements sans réelles conséquences, amendes très rares et généralement faibles).
Cet état de fait participe sans doute du peu d'effectivité de la protection des données personnelles.

Correspondant Informatique et Libertés

Interlocuteur privilégié de la CNIL, nommé dans une organisation (publique ou privée).
Sa présence dispense l'organisation des déclarations (un registre est tenu en interne), pas des demandes d'autorisation.
Le CIL :

- Répertorie les traitements et s'assure qu'ils sont conformes à la loi ;
- Assure l'accès au registre ;
- Dispose d'un contact privilégié à la CNIL, ainsi que d'un réseau ;
- Établit un bilan annuel d'activité, tenu à disposition de la CNIL ;
- A une mission d'assurance qualité, de conseil, de vigilance.

Le CIL deviendra, avec le règlement, un « délégué à la protection des données » (DPD, ou DPO pour *Data Protection Officer*).

Profil-type du CIL

Informaticien, juriste d'entreprise, auditeur, avocat...

Rattachement à l'organigramme lui assurant l'indépendance (idéal : **secrétariat général, DG, présidence**, mais on trouve aussi RH, RSSI, département juridique...

Le futur délégué à la protection des données aura, en plus des missions du CIL, une mission de **contrôle**. Cela implique des moyens et des compétences particulières, ainsi qu'une responsabilité individuelle.

Données personnelles et vie privée au travail

Principe général

Dans le cas général, le salarié a le droit d'utiliser ponctuellement les moyens mis à sa disposition par son employeur pour des fins personnelles.
Il ne doit bien sûr pas en abuser...

L'accès de l'employeur aux e-mails

Arrêt « Nikon » (2001) de la chambre sociale de la Cour de cassation
Si un e-mail est marqué comme personnel, ou classé dans un dossier confidentiel, l'employeur ne peut en prendre connaissance (secret des correspondances).
Dans les autres cas, il y a présomption de caractère professionnel.

Données personnelles et vie privée au travail

L'accès de l'employeur aux fichiers

Arrêt « The Phone House » (2007) de la chambre sociale de la Cour de cassation : extension du principe aux fichiers (y compris la présomption de caractère professionnel).

Arrêt de 2005 : « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

Chambre sociale, 2011 : « Si l'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut les utiliser pour le sanctionner s'ils s'avèrent relever de sa vie privée. »

Données personnelles et vie privée au travail

Arrêt de 2009 : l'administrateur « est tenu d'une **obligation de confidentialité** » (même vis-à-vis de l'employeur) et peut accéder aux données des courriers électroniques échangés par les salariés uniquement « dans le cadre de sa mission de sécurité du réseau informatique ».

Et pour la consultation de sites web ?

À ma connaissance, pas d'arrêt de la Cour de cassation dans ce sens...

L'employeur a, a priori, le droit connaître les sites web consultés par les salariés (et de capturer le contenu des interactions ?).

Données personnelles et vie privée au travail

Géolocalisation des salariés

Particulièrement pertinent pour les sociétés de transport : maintien de statistiques sur les trajets, contrôle des itinéraires...

La CNIL considère que le salarié doit pouvoir désactiver le dispositif à l'issue de son temps de travail.

Attention à la finalité déclarée du traitement : si c'est les stats et l'optimisation, impossible de s'en servir à titre disciplinaire contre le salarié.

Attention également si le salarié dispose de la liberté d'organisation de son temps de travail.

Données personnelles et vie privée au travail

Vidéosurveillance au travail

Finalités autorisées : sécurité des biens et des personnes (dissuasion, identification des responsables)

- **On peut filmer :** entrées et sorties des bâtiments, issues de secours, voies de circulations, zones de stockage de marchandises...
- **On ne peut pas filmer :** employés sur leur poste de travail, zones de pause ou de repos, toilettes, locaux syndicaux et de RP (y compris leur accès).

→ Accès limité (au personnel de sécurité, pas aux RH ou à la direction !)
→ Conservation limitée à **un mois**

Formalités auprès de la CNIL, de la préfecture (suivant les cas), des instances représentatives du personnel.
Chaque employé doit être informé **individuellement**, en sus de l'affichage obligatoire.

Contacter le responsable de traitement

Plus difficile si le responsable de traitement n'est pas situé en France, évidemment.

- Liens et adresses de contact proposés par les responsables (désinscription de listes de diffusion, etc.) ;
- Demande à faire valoir ses droits (d'accès, d'information, de rectification...) : courriers-type sur le site de la CNIL ;
- Recommandé AR nécessaire pour faire courir le délai de deux mois (art. 94 du décret du 20 octobre 2005).

Les moyens de recours

Saisir la CNIL

La saisine peut se faire par tout moyen, y compris par lettre simple.
Le site web de la CNIL peut vous guider dans vos démarches.
La CNIL a deux mois pour réagir et est tenue de vous informer des suites.

Saisir le procureur (ou assigner au civil)

Possible, mais... en court-circuitant la CNIL ? Prenez conseil auprès d'un avocat...

Sanctions

- Sanction administrative de la CNIL : jusqu'à 3 000 000 € ;
- Sanction pénale : jusqu'à 5 ans de prison et 300 000 € d'amende (x5 pour les personnes morales) (art. 226-16 à 226-24 du Code pénal).

Sources et crédits iconographiques

- Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking* (`http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/`), Wired, 6 août 2012 ;
- CNIL, *Ce que change la loi pour une République numérique pour la protection des données personnelles* (`https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles`), 17 novembre 2016.