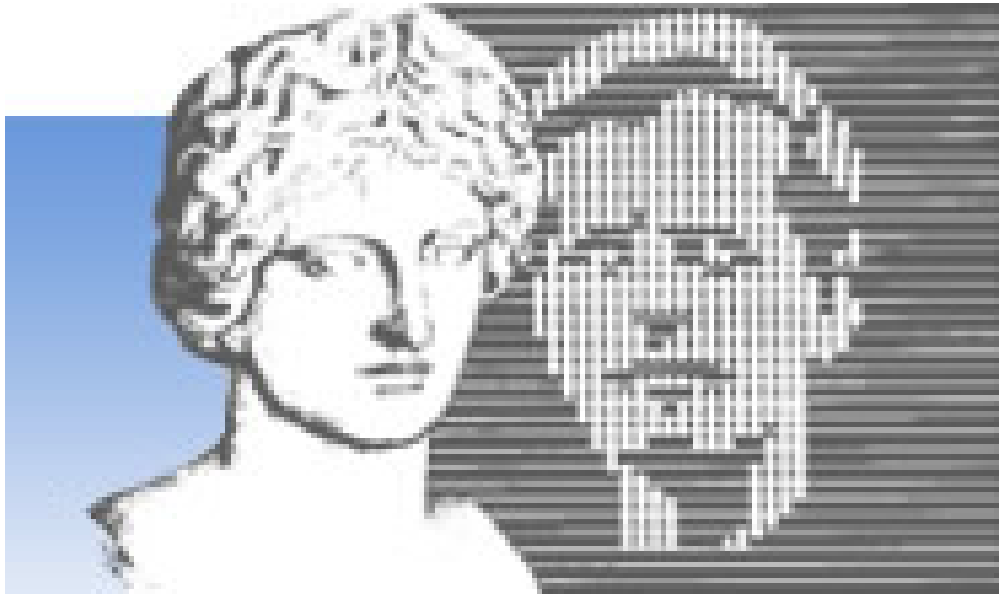
TutoJRES n°7

L'art et la manière de gérer les traces

robert[Pt]longeon[à]cnrs-dir[Pt]fr

01 44 96 48 76 01 44 96 49 95

Retour sur la nouvelle loi CNIL



Une vision plus étendue

Le nouveau cadre législatif s'applique désormais aux "**données à caractère personnel**" et non plus aux "**données nominatives**".

L'article 2 de la loi modifiée définit ainsi 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 ».

Cette définition a l'avantage de ne pas sous-entendre que seules seraient protégées les données liées au nom. En ce qui concerne le traitement de données à caractère personnel dans le domaine de la recherche biomédicale, le régime dérogatoire antérieur est maintenu.

- Le seul fait de collecter des profils de visiteur afin de suivre la fréquentation d'un site web, si cette collecte recueille l'adresse IP des internautes, est un traitement automatisé de données personnelles.
- Le seul fait de mettre sur un site web un forum, un livre d'or qui recueille des adresses électroniques non anonymes, d'utiliser un seul cookie qui récupère l'IP, fait également entrer dans le champ d'application de la nouvelle loi informatique et libertés.

Des conditions de licéité affermies …

Les «conditions de licéité des traitements de données à caractère personnel» (article 6 nouveau) **:**

- être collectées et traitées de manière loyale et licite,
- être collectées pour des finalités déterminées,
- être adéquates, pertinentes et non excessives face à leur finalité,
- être exactes, complètes et mises à jour,
- être conservées en respectant les délais de conservations.

L'accent est mis sur le consentement de la personne concernée par la collecte et le traitement de ses données à caractère personnel (article 7 nouveau).

… et nouvelles !

Obligation d'information élargie :

Auparavant, les personnes auprès desquelles étaient recueillies des informations nominatives devaient seulement :

- être informées du caractère obligatoire ou facultatif des réponses,
- des conséquences d'un défaut de réponse,
- des destinataires des données
- d'un droit d'accès et de rectification.

Dorénavant, elles doivent également être averties :

- des informations relatives à l'identité du responsable du traitement,
- de la finalité poursuivie par le traitement,
- du droit de s'opposer à ce que ces informations soient transférées à des tiers
- des transfert, le cas échéant, de données envisagés vers un État non membre de la Communauté européenne.

Le législateur a prévu également une obligation d'information spécifique en ce qui concerne l'utilisation des dispositifs propres aux services de communications électroniques (ie les "cookies") et une possibilité pour les personnes de s'y opposer.

Des exigences de sécurité affirmées

➔Déclarer un traitement entrant dans le champ de la nouvelle loi est une chose, conserver de manière sûre les fichiers informatiques correspondants en est une autre : **une erreur de sauvegarde entraînant la destruction de données ou une intrusion à l'origine de la divulgation publique d'informations protégées par la loi coûteront chers aux responsables concernés,** y compris s'il s'agit d'une association de passionnés qui fait de l'hébergement libre.

Article 34 nouveau.
Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Article 226-17 du Code Pénal.
Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de **cinq ans d'emprisonnement et de 300 000 euros d'amende**.

Article 50 nouveau.
Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

➔ **Le devoir de secret des ARS et des RSSI**

Article 226-13 du Code Pénal : La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende.

Politique de gestion des traces

La gestion des traces :

Le CNRS a besoin d'enregistrer systématiquement certaines traces générées par les postes de travail, les serveurs, les équipements d'extrémité (routeurs, pare-feux, commutateur, borne d'accès, …), les équipements de surveillance du trafic réseau (IDS, antivirus, antispam, ...), certaines applications spécifiques, etc.

Afin :

- **d'assurer la métrologie du réseau** : réguler l'utilisation des ressources, détecter des anomalies afin de mettre en place de la qualité de service, faire évoluer les équipements en fonction des besoins ;
- **Vérifier que les règles** en matière de SSI sont correctement respectées et que la sécurité des systèmes d'information et du réseau telle qu'elle a été définie par la politique de sécurité de l'unité est assurée ;
- **Détecter toute défaillance** ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ; Détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité du CNRS ;
- **Mettre à l'abri les preuves** nécessaires aux enquêtes en cas d'incident de sécurité et pouvoir répondre à toute réquisition officielle présentée dans les formes légales.

- Quelles sont les responsabilités des ARS et RSSI vis-à-vis de ces traces ?
- Quel soutien organisationnel apporter aux ARS et RSSI pour leur permettre d'assurer leur fonction sans violer leur devoir de secret professionnel ?

Un cadre réglementaire et normatif (1)

La mise en place d'une **politique de gestion des traces** "déclarée à la CNIL" a d'abord pour objectif d'offrir aux ARS et aux "correspondants sécurité" le cadre réglementaire et normatif dont ils ont besoin. Tout d'abord :

Elle spécifie :

- quelles sont les types de trace qui sont licites de conserver et pendant quelle durée,
- les finalités de traitement auxquels elles donneront lieu,

et rappelle les principes

- d'information préalable,
- du droit à consultation,
- du non détournement de finalité
- du droit à l'oubli.

Un cadre réglementaire et normatif (2)

Elle précise ensuite les règles et les procédures pour que :

- La collecte des informations ne soit ni frauduleuse, ni déloyale, ni illicite et qu'elle s'accompagne d'une bonne information des personnes ;
- Les informations ne soient pas conservées au-delà de la durée prévue ;
- Les informations ne soient pas communiquées à des personnes non autorisées ;
- Les traitements ne fassent pas l'objet de détournements de finalité ;
- L'accès aux résultats des traitements et aux données collectées fasse l'objet d'une sécurité optimale.

Chaîne fonctionnelle de la SSI

A qui transmettre l'information ?

Chaîne fonctionnelle

SGDN

Haut Fonctionnaire de Défense et de Sécurité

Chaîne hiérarchique

Directeur Général du CNRS

FSD

Départements scientifiques

Chargé de Mission SSI (CMSSI)

Délégués régionaux

Réseau des Coordinateurs régionaux SSI (CRSSI)

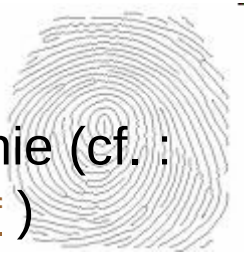
Autres tutelles

Entités/laboratoires

Réseau des Chargés de SSI (CSSI)

Conclusion

Deux attitudes possibles :



1°) La politique de gestion des traces telle qu'elle a été définie (cf. : https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/Po_gest_traces.pdf)
vous convient : il n'y a rien d'autre à faire … sinon respecter scrupuleusement les règles (en particulier celles se référant à l'information des utilisateurs)

2°) La politique de gestion des traces ne vous convient pas : il faut en déclarer une autre à la CNIL. On pourra partir du texte existant.

Merci !

Questions ?