Les traces et logs
Législation - Réglementation

Bernard Martinet

Coordination SSI Université de Grenoble

Quelques termes

- Codes
- Loi
- Décret
- Décret d’application
- Arrêté
- Circulaire

Quelques termes (2)

- Jurisprudence :
  - Ensemble des arrêts et des jugements rendus par les Cours et les Tribunaux pour une situation juridique donnée.
  - Décisions illustrant un problème juridique
  - Habitude de juger
  - Revirement possible

Codes et Lois des NTIC*

- Code de la propriété intellectuelle
- Code pénal
- Code civil
- Code du travail
- Code des postes et des communications électroniques

*origine www.celog.fr

Codes et Lois des NTIC (2)

- Loi Godfrain du 05/01/88 sur les Systèmes de Traitement Automatiques de Données.
- LCEN (Loi pour la confiance dans l'économie numérique n° 2004-575 du 21/06/2004)
- Loi n° 2004-801 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (modif loi n° 78-17 du 06/01/76 dites informatique et libertés)
- Loi du 1er août 2000 modifiant la loi du 30 septembre 1986 relative à la liberté de communication:
- Articles 43.7 à 43.10 (sur les services de communication en ligne autres que de correspondance privée)
- Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle
- Loi DADVSI (03 Août 2006)
- Loi HADOPI 2 (décret d'application 31 Dec. 2009)
- Loi LOPPSI 2 (15 Mars 2011)

Les Différents statuts de l'internet

- Statuts définis légalement (LCEN)
- Fournisseur d’accès
- Hébergeurs
- Éditeur de contenu
- Opérateur de communication électronique

Fournisseur d'accès

- Entreprise offrant un accès au réseau internet
- Exonéré de toutes responsabilités
- Obligations
  - Information à l'autorité sur toutes activités illicites alléguées.
  - Information des abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains sites ou de les supprimer.
  - Conservation des moyens d'identifier les usagers de leurs services
  - Réponse à une demande des autorités de couper l'accès à certains sites.

Hébergeur

- Personne ou société mettant à disposition des internautes des sites web conçus et gérés par des tiers.
- Pas de responsabilité sur les contenus
- Obligations
  - Bloquer les sites comportant des contenus à caractères racistes ou pédopornographique.
  - Intervenir promptement lors d'avertissement de tous contenus illicites.

Éditeur de contenu

- Personne ou société qui met à la disposition du public des pages sur internet.
  - Sélection du contenu, assemblage, hiérarchisation, mise en forme du support…
- Obligations
  - Surveiller les contenus de son site
  - Publication de la réponse d'une personne nommée ou désignée sur un site (cf. loi sur la presse)

Éditeur de contenu (2)

- Responsable de ce qu'il écrit ou met en ligne dans tous les cas prévus dans la loi sur la presse
  - Conseil constitutionnel : L'éditeur d'un site internet comprenant un espace de contributions personnelles et ayant mis en place un système de modération a priori peut potentiellement voir sa responsabilité engagée à raison des messages publiés, sauf à désigner l'auteur ou démontrer que le directeur de la publication est responsable.
- Besoin d'une politique éditoriale rigoureuse !

Opérateur de communication électronique

- Entité qui met à la disposition du public des services de communications à distance → déclaration à l'ARCEP
- Dans certain cas, pas de déclaration à l'ARCEP
  - Ex : Un hôtelier qui gère lui-même son WiFi ouvert à sa clientèle EST un opérateur de communication électronique.
  - Pas de déclaration, mais obligation des FAI en termes de conservation des données par exemple

Traces et Logs : Qui ? Quoi ?

- Définitions
  - Article 6 de la LCEN
  - Code des Postes et communications électroniques + Loi anti-terroriste Sarkozy
  - Les entreprises seraient donc concernées

Obligation de traces

- Jurisprudence BNP Paribas.
  - Dans un arrêt du 3 février 2005, la cour d'Appel de Paris condamne BNP Paribas pour défaut de production de traces.

Durée de rétention

- Plusieurs textes parfois contradictoires
  - Directive européenne : 1 à 2 ans
  - L'article 6 de la LCEN : 1 an
  - La loi anti-terrorisme : 1 an
  - CNIL : 6 mois

- conservation pendant 1 an 

Traces à l'Université

- **Politique type de gestion des journaux informatiques**
  - Document issu des travaux d'un groupe mandaté par la CPU et le MESR
  - Visé par la CNIL
- **Document validé en comité de sécurité opérationnel (SSI inter-U) dec 2011**
  - Validé ou en cours de validation dans les divers établissements

Pourquoi ?

- Métrologie
- Sécurité
- Respect des politiques SSI
- Avoir les preuves nécessaires en cas de réquisition judiciaire

Combien de temps ?

- Conservation des traces
  - La durée de conservation des journaux informatiques est de 1 an maximum.
  - 3 mois en clair : exploitation
  - 9 mois en accès réservé uniquement sur réquisition

Qualités des informations

- Informations journalisées factuelles et contextuelles ;
- importance de l'heure de relève ;
- synchronisation des serveurs sur un serveur de temps ;
- d'éventuelles interruptions de la journalisation doivent être repérables par les destinataires de ces données.

Quoi ? Les serveurs

Les serveurs :

- identifiant de l'émetteur de la requête (login, adresse IP, adresse Ethernet...),
- date et heure de la tentative,
- résultat de la tentative (succès ou échec),
- commandes passées.

Quoi ? La messagerie

La messagerie, les forums… :

- adresse de l'expéditeur,
- adresses des destinataires,
- date et heure,
- Machines traversées,
- le traitement (accepté ou rejeté),
- la taille du message,
- certaines en-têtes (identifiant numérique de message),

Quoi ? La messagerie (2)

...

- résultat du traitement des spams,
- résultat du traitement antiviral,
- validation ou rejet par les modérateurs si nécessaire.

► Les éléments de contenu des messages, notamment le sujet ou l'objet, ne sont pas journalisés.

Quoi ? Web local

Serveurs Web locaux

- noms ou adresses IP source et destination,
- données d'authentification si pertinent (intranet par exemple),
- URL de la page consultée et informations fournies par le client,
- type de la requête,
- date et heure,
- volume de données transférées,
- paramètres passés.

Quoi ? Proxy web

Proxies web

- noms ou adresses IP source et destination et les différentes données d'identification,
- l'URL de la page consultée le type de la requête,
- date et heure,
- volume de données transférées.

Limitations

- Article L.34-1 du codes des postes et télécom ;
- Assimilation du service réseau d'un établissement à un opérateur de communication électronique.

Quoi ? Équipements réseaux

Les équipements réseaux

- noms ou adresses IP source et destination,
- numéros de port source et destination et protocole,
- la date et l'heure,
- traitement du paquet,
- nombre de paquets nombre d'octets transférés,
- messages d'alerte.

► A faire au minimum sur l'accès Internet

Quoi ? Autres applications

Autres applications :

- accès aux bases de données ;
- ENT ;
- Authentification (SSO, LDAP, Radius…).

► les informations suivantes sont collectées :

- identité de l'émetteur de la requête,
- date et heure,
- résultat de la tentative,
- volumes de données transférées,
- commandes passées.

Pour Qui ?

- Les administrateurs systèmes et réseaux
  - Accès aux données de moins de 3 mois
  - Chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau
  - Rapport sur toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau
  - Fourniture d'information uniquement à la demande de la chaîne fonctionnelle de sécurité

Pour Qui ? (2)

- La chaîne SSI
  - les correspondants ou chargés de sécurité des systèmes d'information
  - le responsable de la sécurité des systèmes d'information (RSSI)
  - l'autorité qualifiée de sécurité des systèmes d'information (AQSSI) : Président d'Université, Directeur d'Institut...
  - le fonctionnaire de sécurité de défense (FSD)*
  - tenus au devoir de discrétion professionnelle ou de secret professionnel en fonction de leur mission.

* Le Directeur Général des Services ou tout autre personne officiellement désignée à ce poste

Déclaration CNIL

- Les traces comportant la plupart du temps des données à caractères personnel, celles-ci doivent-être déclarées à la CNIL.
- C'est le cas de la politique de gestion de traces dans les divers établissement du PRES
  - Fait ou en cours d'enregistrement suivant les établissements
- Si vous gérez des traces autres que celles prévues, vous devez faire une déclaration CNIL (voir RelaisCIL@<etab>.fr)

Cas du CNRS

- Le CNRS dispose également d'une politique de gestion de trace déclarée à la CNIL en 2004 pour l'ensemble de ses structures.
- La politique est très proche de celle des universités de Grenoble et Savoie.