



OSSIR
Groupe de travail

**Livre blanc sur les
logs**

Date de publication : 06 novembre 2009

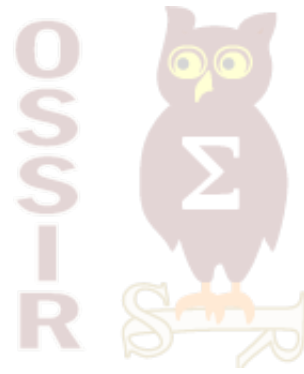
<http://www.ossir.org>





Table des matières

Préface	i
1 Introduction	1
2 Le groupe de travail	2
3 Définition des logs et des traces	3
4 Référentiel légal	4
5 Usages et besoin	5
6 Acteurs impliqués	7
7 Thématiques spécifiques	9
8 Conclusions	11
A Présentation des annexes	13
B Présentation des membres du groupe de travail	14
C Le point de vue de la Cnil	22
D La politique type de gestion des journaux informatiques du Comité Réseau des Universités	24



Préface

Les logs sont utilisés quotidiennement par les administrateurs des systèmes et des réseaux ainsi que les acteurs de la sécurité informatique depuis bien longtemps, mais cela fait peu de temps qu'ils ont investi le monde des juristes. L'apparition en filigrane de références, souvent indirectes dans les textes, a créé un flou artistique autour de l'objet « log ». Il est devenu nécessaire de faire un point et de confronter les points de vue techniques et juridiques pour préciser et affiner l'objet en question.

L'OSSIR (Observatoire de la Sécurité des Systèmes d'Information et des Réseaux) semblait être un cadre idéal pour effectuer une convergence. Les discussions ont comblé les attentes des deux organisateurs, par la richesse des débats, l'atmosphère de convivialité et l'implication des participants.

Pour tout cela nous remercions chaleureusement tous les membres du groupe.

Christophe Labourdette

Docteur en Mathématiques

Ingénieur de recherche

CMLA, UMR 8536 CNRS/Ecole

Normale Supérieure de Cachan

Vice-Président de l'OSSIR

Éric Barbry

Avocat

Directeur du pôle Droit du Numérique

Alain Bensoussan Avocats

Membre de l'OSSIR

Président d'honneur de Cyberlex

Chapitre 1

Introduction

Les logs posent un grand nombre de questions.

Aux hommes de l'art, d'une part, qui s'interrogent de manière récurrente autour des questions suivantes :

- faut-il logger ?
- que peut-on logger ?
- qui peut-on logger ?
- que faire des logs ?

Aux juristes, d'autre part, qui se posent d'autres questions :

- qu'est-ce qu'un log ?
- à quoi peuvent servir les logs ?
- comment s'assurer de leur caractère probant ?
- sont-ils des données personnelles ?
- quels dangers peuvent-ils représenter ?

Il est apparu que si les questions semblaient de prime abord distinctes, elles ne pouvaient être traitées que conjointement, les réponses des uns impactant nécessairement celles des autres.

C'est pourquoi l'OSSIR, a créé un groupe de travail destiné à s'interroger sur la problématique des logs. Ce groupe de travail est original dans sa composition, l'objectif étant qu'il regroupe à parité des experts techniques de la matière, d'une part, et des juristes et avocats, d'autre part.

Chapitre 2

Le groupe de travail

Le groupe de travail a été co-présidé par Christophe Labourdette, Ingénieur de recherche au CNRS, vice-président de l'OSSIR et Eric Barbry, avocat associé au sein du Cabinet Alain Bensoussan, membre de l'OSSIR et président d'honneur de Cyberlex.

Le groupe de travail est composé de :

- Jacqueline Fortuné ;
- Florence Grisoni ;
- Anne Mur ;
- Martine Ricouart Maillet ;
- Serge Aumont ;
- Bruno Méline ;
- Nicolas Reymond ;
- Raphael Marichez.

Le groupe de travail a défini un programme de réflexion autour des principaux axes suivants :

- la définition des logs ;
- les usages et les besoins ;
- les acteurs impliqués ;
- un ensemble de thématiques :
 - données personnelles ;
 - preuve ;
 - archivage ;
 - propriété ;
 - responsabilité.

Le groupe s'est fixé un mode opératoire particulier :

- un nombre limité de membres ;
- une participation active desdits membres ;
- un nombre limité de réunions ;
- la réalisation, à la suite des réunions, d'un travail de synthèse.

Chapitre 3

Définition des logs et des traces

Le terme « log » provient de la langue anglaise (journal de bord des navires). Il est notamment employé en informatique pour désigner un historique d'événements et par extension le fichier contenant cet historique. Le terme « log » en tant que tel n'apparaît pas dans la réglementation française. Les textes applicables, qu'il s'agisse de textes nationaux ou de directives communautaires, retiennent les termes suivants :

- « données relatives au trafic »¹ ;
- « données de nature à permettre l'identification »² ;
- « données de connexion à des services de communications électroniques »³ ;
- « données de connexion »⁴ ;
- « fichiers de journalisation des connexions »⁵.

Le groupe de travail estime que l'absence de définition du terme « log » sur un plan juridique et l'absence de clarté des termes utilisés rend le droit des logs difficilement compréhensible. Le groupe de travail considère que pour une meilleure compréhension il est nécessaire de distinguer les « logs » des « traces » et propose les définitions suivantes :

- « log » : journalisation de données informatiques résultant de l'utilisation d'une application ;
- « trace » : donnée informatique témoignant de l'existence d'une opération au sein d'une application.

En effet, si toute utilisation d'une application induit directement ou indirectement des « traces », les « logs » eux-mêmes sont le résultat d'un choix volontaire du concepteur ou de l'utilisateur de surveiller une application.

De fait, tout log contient des traces mais toute trace n'est pas nécessairement dans un log. Les logs possèdent en effet quelques caractéristiques qui les différencient des traces :

- leur structure est précise et connue, elle permet un traitement automatisé ;
- ils sont datés ;
- les événements sont inscrits dans le journal au moment même où ils surviennent.

¹ Art. L. 34-1 et R.10-12 et suivants du Code des postes et des communications électroniques.

² Art 6-II de la loi pour la confiance dans l'économie numérique du 21-6-2004.

³ Art. L. 34-1-1 du Code des postes et des communications électroniques.

⁴ Fiches de synthèse « Cybersurveillance sur les lieux de travail » du 11 février 2002 de la Cnil.

⁵ Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition 2004.

Guide de la Cnil « Guide pratique pour les employeurs et les salariés », édition 2008.

Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition 2004.

Guide de la Cnil « Guide pratique pour les employeurs et les salariés », édition 2008.

Chapitre 4

Référentiel légal

Le présent livre blanc s'inscrit dans le cadre d'un référentiel légal constitué notamment des textes suivants :

- directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques ;
- directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications ;
- articles L. 34-1 et s. et R.10-12 et s. du Code des postes et des communications électroniques ;
- article L. 335-12 du Code de la propriété intellectuelle ;
- loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et ses modifications ;
- loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ;
- loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Il tient compte également de l'état de la jurisprudence et notamment de l'arrêt de la chambre sociale de Cour de cassation du 9 juillet 2008, selon lequel :

« les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence »¹.

¹Cass. soc. 9-7-2008 pourvoi n°06-45800.

Chapitre 5

Usages et besoin

Le groupe de travail a constaté qu'il existait a priori une différence entre les usages, les besoins des hommes de l'art et ceux des juristes :

- Pour l'homme de l'art, le log a pour usage principal de surveiller et contrôler les conditions d'utilisation d'une application ;
- Pour les juristes, les logs sont utilisés comme un moyen de preuve.

Le groupe de travail s'est tout d'abord interrogé sur le droit ou non de surveiller et de contrôler l'utilisation d'une application informatique.

Il existe en effet une ambiguïté qui consiste à permettre, voire à obliger les personnes juridiquement responsables (employeur vis-à-vis de leurs employés, parents vis-à-vis de leurs enfants, enseignants vis-à-vis des apprenants) à contrôler les personnes qui répondent d'elles, tout en imposant un grand nombre de limites à ce « droit de contrôle ».

Au rang des limites figurent notamment :

- les principes de légitimité,
- de proportionnalité,
- de non-discrimination,
- de protection de la vie privée.

La jurisprudence témoigne d'ailleurs de cette difficulté qui, dans certains cas, a abouti à la condamnation des employeurs pour défaut de contrôle¹ et, dans d'autres, a débouché à leur condamnation pour avoir mis en œuvre des moyens de contrôle².

Le groupe de travail préconise donc que soient clarifiées les conditions dans lesquelles peuvent être déployées des solutions de contrôle et de surveillance.

Le groupe s'est également interrogé sur le caractère probatoire des logs. Il est manifeste que les logs sont aujourd'hui utilisés à titre probatoire, dans le cadre de précontentieux comme dans le cadre de contentieux. Généralement, les logs ainsi produits ont été admis à titre de preuve. Les logs posent néanmoins une véritable problématique en terme de recevabilité du fait que souvent, les conditions dans lesquelles ils sont conservés ne permettent pas d'en assurer l'origine, l'authenticité et l'intégrité.

¹CA ch. 2e Aix-en-Provence du 13-3-2006 n°2006/170 SA Lucent c. / SA Escota SA Lycos Nicolas B.

²Cass. Soc. 2-10-2001 n° 99-42942.

Il est donc nécessaire de reconnaître, et ce de manière incontestable, la valeur juridique et probatoire des logs et, le cas échéant, de fixer les meilleures pratiques assurant leur recevabilité à titre de preuve.

Chapitre 6

Acteurs impliqués

Le groupe de travail a pu distinguer trois grands types d'acteurs :

- les personnes qui sont, de par la loi, tenues de mettre en œuvre, détenir et conserver des logs ;
- les personnes qui sont soumises à une obligation de contrôle de tiers et qui vont, de ce fait, utiliser les logs comme un moyen d'exercer ce contrôle ;
- les personnes qui « manipulent » les logs et sont généralement des personnes disposant d'un droit d'administration sur une application.

S'agissant en premier lieu des personnes qui sont, de par la loi, tenues de mettre en œuvre, de détenir et de conserver des logs figurent les opérateurs de communications électroniques. Ces opérateurs sont notamment visées par l'article L.34-1 du Code des postes et communications électroniques.

En réalité, cette obligation pèse sur de très nombreux acteurs puisque l'article L.34-1 du Code prévoit que :

« Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »

Cette obligation ne vise donc pas uniquement les opérateurs de communications électroniques au sens strict du terme. Figurent également dans cette catégorie les autorités policières ou judiciaires disposant du droit de procéder à des opérations de contrôle et de surveillance.

En second lieu, concernant les personnes tenues à une obligation de contrôle à l'égard de tiers se trouvent notamment :

- les employeurs vis-à-vis de leurs préposés ;
- les parents vis-à-vis de leurs enfants ;
- ou encore les enseignants vis-à-vis des apprenants.

Au plan civil, il est en effet nécessaire rappeler les règles posées par l'article 1384 du Code civil qui dispose que :

« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. [...] »

Ainsi les pères et les mères, du fait qu'ils exercent l'autorité parentale, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux. De même que les commettants sont responsables du dommage causé par leurs préposés dans le cadre de l'exercice des fonctions pour lesquelles ils ont été employés.

A côté de la question de la responsabilité civile, se pose naturellement celle de la responsabilité pénale. L'article 121-1 du Code pénal dispose que :



« nul n'est responsable que de son propre fait ».

Ainsi, par exemple, un employeur ne devrait pas être responsable des fautes pénales commises par ses employés. Il convient cependant de tempérer cette position de principe en se référant à l'article 121-2 du Code pénal qui, pour sa part, dispose que :

« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants. »

Ces deux sphères de la responsabilité civile ou pénale induisent la nécessité de mettre en œuvre des mesures de contrôle.

Enfin, au titre des personnes qui « manipulent » les logs figurent celles qui disposent d'un droit d'administration sur une application. Contrairement aux deux catégories précédentes, les personnes qui « manipulent » les logs ne bénéficie d'aucun cadre légal spécifique. Les règles qui pourraient leur être applicables relèvent de :

- la jurisprudence¹ ;
- la documentation de la Cnil, qui a pris position concernant les rôles et responsabilités des administrateurs, dans plusieurs de ses rapports².

De son côté, le Forum des droits sur Internet présente la position suivante :

« Le Forum recommande la mise en place d'un statut particulier pour l'administrateur réseau au sein de l'entreprise [...] ».

Dans ce contexte, le groupe de travail s'inquiète de cette situation source d'insécurité juridique.

Le groupe de travail préconise que soit adopté un statut juridique protecteur des personnes disposant de droits d'administration sur un système d'informations, à l'instar de ce qui existe pour d'autres catégories de personnes ou d'autres fonctions comme celle de Cil (correspondant informatique et libertés) ou de déontologue.

¹CA Paris 4-10-2007 22e ch. sect. C.

CA Paris 11e ch. 17-12-2001 Françoise V., Marc F. et Hans H. / ministère public, Tareg Al B.

²Fiches de synthèse « Le rôle des administrateurs de réseaux », du 11-2-2002 de la Cnil.

Rapport de la Cnil « La cybersurveillance sur les lieux de travail », édition 2004.

Guide de la Cnil « Guide pratique pour les employeurs et les salariés », édition 2008.

Chapitre 7

Thématiques spécifiques

Le groupe de travail s'est par ailleurs penché sur la question de la compatibilité ou la cohérence de la notion de log avec un ensemble d'autres paramètres juridiques :

- les logs et les données personnelles,
- les logs et le droit de la preuve,
- les logs et la responsabilité,
- les logs et la propriété,

ont été quelques unes des questions débattues.

Sur la question des logs et du droit des données à caractère personnel, le groupe de travail estime que, dans la mesure où l'objectif juridique premier des logs est d'apporter la preuve de :

- l'utilisation,
 - ou de la non-utilisation d'une application informatique par un utilisateur,
- ceux-ci ne sont exploitables que s'ils permettent effectivement d'identifier directement ou indirectement un individu. Les logs comportent en ce sens des données à caractère personnel. De fait, la mise en œuvre de logs impose donc le respect de la loi du 6 janvier 1978 modifiée, qui implique notamment :
- l'existence de formalités préalables auprès de la Cnil (déclaration, autorisation...);
 - le respect des droits des personnes (information, consentement, droit d'accès, droit de rectification, droit à l'oubli, droit à l'anonymat...);
 - la mise en œuvre d'un niveau adapté de sécurité;
 - la gestion juridique des éventuels flux transfrontaliers;
 - la gestion de l'archivage.

Les logs ne pourront être conservés que dans des délais précis, sauf à mettre en œuvre des techniques d'anonymisation. Il convient cependant d'être prudent en matière d'anonymisation dans la mesure où, si l'anonymisation est « réelle » c'est-à-dire non réversible, le log perd sa capacité probatoire s'agissant de l'identification des utilisateurs. Par ailleurs, si les logs ont par nature un objectif probatoire, afin d'être opposables en cas de contentieux, ils doivent respecter les règles relatives à l'administration de la preuve. Parmi ces règles, figurent notamment les obligations en terme d'identification et d'intégrité. L'acquisition et l'usage des logs doivent ainsi s'effectuer dans le respect de la loi (Informatique et libertés, droit du travail, droit pénal...).

En termes de responsabilité, les logs posent essentiellement cinq types de difficultés :

- la responsabilité de ne pas logger;
- la responsabilité du fait de logger;
- la responsabilité du fait de détenir ou conserver des logs;
- la responsabilité de prendre connaissance et/ou de communiquer des logs.



- la responsabilité du fait de l'altération et/ou de la modification des logs ;

Sur le premier point, il convient de rappeler qu'il existe pour certaines catégories ou acteurs juridiques une obligation de détention et de conservation des logs. Ne pas logger implique pour eux de ne pas respecter une obligation légale¹, punie d'un an d'emprisonnement et de 75000 euros d'amende².

La question se pose pour tous les autres acteurs qui ne relèvent pas d'un régime d'obligation. Il est nécessaire de rappeler que, parmi les fondamentaux de la responsabilité, figure la responsabilité pour « négligence fautive ». Il est donc à craindre, au regard de l'état de l'art en la matière, que le fait de ne pas logger et donc de ne pas être en mesure de prouver, pourrait être considéré comme constitutif d'une négligence.

La responsabilité du fait de logger peut pour sa part être appréhendée sous deux angles :

- le non-respect de la loi quant à l'acquisition et l'exploitation des logs, d'une part ;
 - la mauvaise interprétation des logs, qui aurait conduit à sanctionner par erreur un utilisateur, d'autre part.
- Pourra également voir sa responsabilité engagée celui qui détient des logs sans droit ni titre ainsi que celui qui les lui a communiqués. Enfin, sur un plan pénal, l'altération et/ou de la modification des logs pourraient conduire à l'application de l'article 323-3 du Code pénal qui dispose que :

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. »

Par ailleurs, le groupe de travail s'est interrogé sur la propriété même des logs et a considéré que, par principe, les logs étaient la propriété du loggateur et non du loggué. Il convient cependant de préciser que le loggateur technique n'est pas nécessairement le loggateur juridique. Tel est le cas en matière de sous-traitance. De fait, dans une telle hypothèse, il importe de gérer la propriété des logs dans le contrat qui lie le client au fournisseur.

¹ Art 6-II de la loi pour la confiance dans l'économie numérique du 21-6-2004.

² Art 6-VI-1° de la loi pour la confiance dans l'économie numérique du 21-6-2004.

Chapitre 8

Conclusions

Le groupe de travail propose les définitions suivantes des termes « log » et « trace » :

- « log » : journalisation de données informatiques résultant de l'utilisation d'une application ;
- « trace » : donnée informatique témoignant de l'existence d'une opération au sein d'une application.

Le groupe de travail a pu constater que :

1. les logs sont l'exemple type de la convergence de la technique et du droit ;
2. les logs n'ayant pas de statut juridique propre, ils apparaissent de manière plus ou moins claire dans l'arsenal juridique, ce qui n'est pas sans poser des difficultés en termes de sécurité juridique ;
3. les logs sont pourtant d'ores et déjà utilisés dans le cadre de pré-contentieux ou de contentieux comme éléments de preuve admis par la Cour de cassation elle-même ;
4. aucun log ne peut être mis en œuvre sans le respect de la loi.

Le groupe de travail estime nécessaire :

- la création d'un statut juridique des logs ;
- la mise en œuvre de logs dans le cadre d'une politique de gestions de logs qui repose sur les quatre composantes suivantes :
 - conformité ;
 - référentiel ;
 - sensibilisation ;
 - audit.

La conformité s'entend essentiellement par rapport à la loi (aspect juridique) d'une part et à l'état de l'art (aspect technique) d'autre part.

Le référentiel relève de la nécessité de définir, écrire et rendre opposables les règles relatives à la création, l'acquisition, la conservation et l'utilisation des logs. Ce référentiel dépend évidemment de chaque structure (sensibilité, nombre de personnes, nombre d'applications, etc.). Ce référentiel pourra prendre la forme de mentions au sein de chartes des personnels relatives à l'utilisation des moyens informatiques et de communications électroniques, de chartes « administrateurs », d'une politique des logs, de politiques ou schémas directeurs de sécurité, de guides d'administration de la preuve, de politiques d'archivages, de notes de service, etc. Ces référentiels devront nécessairement traiter la problématique particulière des personnes susceptibles de « manipuler » les logs et de leur protection, qui sont en particulier les administrateurs systèmes et réseaux.

La sensibilisation s'impose en matière de logs : il s'agira d'informer et sensibiliser l'ensemble des personnels, en portant à leur connaissance les référentiels et en complétant cette information par des formations, à minima destinées aux administrateurs.

Enfin, s'agissant de l'audit et du contrôle, ils s'avèrent en l'espèce indispensables du fait des risques juridiques liés au respect ou non des obligations légales et des éléments du référentiel de chaque structure.

Annexe

Présentation des annexes

Le présent Livre blanc comprend trois annexes :

- annexe **B** : Présentation des membres du groupe de travail ;
- annexe **C** : Le point de vue de la Cnil ;
- annexe **D** : La politique type de gestion des journaux informatiques du Comité Réseau des Universités, version 2.6 novembre 2008 accessible via le lien : http://www.cru.fr/activites/securite/index#gestion_des_traces.

Annexe B

Présentation des membres du groupe de travail

Certaines personnes du groupe de travail n'ont pas souhaité faire figurer leur curriculum vitæ dans le livre blanc, la présentation est donc incomplète.



Eric Barbry, Avocat au Barreau de Paris

Directeur du Pôle « Droit du numérique »

Eric Barbry dirige le pôle « Droit du numérique » du Cabinet Alain Bensoussan constitué d'une équipe de 20 avocats. Ce pôle regroupe les départements « Internet Conseil », « Internet Contentieux », « sécurité des systèmes d'information », « Informatique & libertés privé », « informatique et libertés public » et « marketing & publicité électronique ». Il est l'auteur de plusieurs ouvrages et articles consacrés au droit de l'Internet et du numérique. Il est membre fondateur de Cyberlex et de l'Association française des correspondants informatique et libertés. Membre de l'OSSIR. Il est chargé d'enseignement à Telecom ParisTech.



Tél : 01 41 33 35 35 – **Fax :** 01 41 33 35 36 - **Portable :** 06 13 28 91 28

Adresse mail : eric-barbry@alain-bensoussan.com



ALAIN BENSOUSSAN SELAS

29, rue du Colonel Pierre Avia – 75508 Paris Cedex 15

<http://www.alain-bensoussan.com>

Equipe : 120 personnes

Créé en 1978, le cabinet s'est orienté, dès l'origine, vers le droit de l'informatique. Autour de son cœur de métier constitué par l'informatique et les communications électroniques, il se consacre, tant en conseil qu'en contentieux, à de nombreux secteurs relevant des technologies avancées, associant la connaissance de ce secteur technique et du droit spécifique qui s'y applique, à celle des grandes catégories du droit. Il met l'accent sur les stratégies innovantes et l'élaboration de concepts nouveaux anticipant sur les questions de droit générées par le développement des nouvelles technologies. Installé à Paris, le cabinet s'est développé en région avec un bureau secondaire à Lyon et à Grenoble.

L'équipe, composée d'avocats et de juristes, apporte son savoir-faire suivant les quatre axes de l'exercice de son métier :

- contrat et pilotage de projet ;
- conseil, audit et assistance juridique ;
- précontentieux, contentieux et arbitrage ;
- infogérance juridique.

Il est privilégié une approche concrète des dossiers grâce à une connaissance approfondie des techniques et des métiers.



Anne MUR

Responsable du pôle sécurité du Groupe ON-X / EdelWeb

Conseil

Expérience de plus de 15 ans en assistance à maîtrise d'ouvrage en Sécurité des Systèmes d'Information et dans la conduite de nombreuses missions de SSI dans les secteurs de la banque, de l'assurance, des services, de l'administration et de l'industrie pour des missions concernant en particulier les domaines de compétences suivants :

- Assistance à l'élaboration de Systèmes de Management de la Sécurité de l'Information et à sa mise en œuvre ;
- Définition de politiques de sécurité, analyses de risques, audits de sécurité ;
- Assistance à l'élaboration et à la mise en place de plans de sécurité ;
- Spécifications de sécurité, et assistance au choix de solutions organisationnelles et techniques pour la protection du SI ;
- Assistance à maîtrise d'ouvrage pour l'élaboration de Plans de Continuité d'Activité ;
- Formation / Sensibilisation : Conception et animation de séminaires de sensibilisation à la Sécurité des Systèmes d'information, ;
- animation de conférences ;
- Veille sécurité dans les domaines : Juridiques, réglementaires, méthodes, normes, standards, technologies, menaces, vulnérabilités.



Expertise SSI

- Méthodologies SSI : EBIOS, MEHARI, Méthode de Défense en profondeur ;
- Application des standards et normes tels que ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO15408. Certifiée Lead Auditor ISO27001 ;
- Expertises dans les domaines liés aux réseaux d'entreprise et particulièrement concernant la protection des environnements utilisateurs de travail et la lutte contre les codes malveillants.

Expertise SSI

- Animation de nombreuses conférences et formations sur plusieurs thèmes de la sécurité ;
- Membre du club EBIOS, animatrice du club 27001 toulousain ;
- Chargée de cours à l'Université des Sciences Sociales de Toulouse depuis 1995.

Tél : 01.40.99.14.14 - **Portable :** 06.86 46 19 35

Adresse mail : anne.mur@edelweb.fr



Christophe LABOURDETTE, Ingénieur

Ingénieur de recherche Centre de Mathématiques et de Leurs Applications (CMLA), UMR 8536 CNRS/ENS-CACHAN. Docteur en mathématiques de l'université d'Orsay.

Responsabilités diverses :

- 1993-2009 : Responsable informatique du CMLA ;
- 2001-2003 : Direction du projet « La forge est avec toi ! » labellisé par le réseau de Recherche et d'Innovation en Audiovisuel et Multimédia (RIAM) ;
- 2001-2009 : Adjoint à la direction du parcours, Méthodes Numériques pour les Modèles des Milieux Continus (MN2MC) du Master de Mathématique de l'ENS de Cachan ;
- 1997-2005 : Rssi adjoint de l'ENS de CACHAN pour le Comité Réseau des Universités ;
- 1997-2009 : Président ou vice-président de l'Observatoire de la Sécurité des Systèmes d'Information et des Réseaux (OSSIR).



Enseignements dispensés, aux élèves de l'ENS de Cachan, ainsi qu'aux élèves de deuxième année des masters Modélisation et Simulation (INSTN) et MN2MC, autour des thèmes suivants : Unix et Linux, programmation scientifique objet, langages scripts, calcul scientifique, optimisation de code, C, C++, Java, Matlab, Python, LaTeX.

Thèmes de recherche et pôles d'intérêts :

- Les nouvelles technologies de l'enseignement scientifique, programmation objet et calcul scientifique ;
- Applications Web, simulation numérique, optimisation de code, IHM et calcul scientifique, développement et sécurité, génie logiciel, sécurité des systèmes et des réseaux informatiques, cryptographie et signature numérique ;
- Théorie de l'information et apprentissage statistique, réseaux sociaux.
- Modélisation et simulation en mécanique des fluides.



Bruno MELINE, Ingénieur

Titulaire d'un DEA de Gestion Paris-Dauphine et d'une maîtrise de sciences politiques et juridiques

Ses activités s'exercent comme :

- Expert auprès de l'Union Européenne ;
- Spécialiste en sécurité des systèmes d'information ;
- Consultant Senior au sein d'un grand groupe informatique ;
- Enseignant en sécurité des systèmes d'information ainsi qu'en gestion de l'entreprise.

Tél. portable : 06.07.60.41.32

Adresse mail : bmeline@meline.org





Florence GRISONI, Juriste Chercheur

Juriste Chercheur EADS France Innovation Works

Experte en droit de la Sécurité des Systèmes d'Information et en droit du numérique.

Florence Grisoni est Juriste au département recherche d'EADS France dans une équipe de chercheurs en sécurité informatique et sécurité des Systèmes d'information qu'ils soient embarqués ou non.

Son domaine d'expertise entre technique et juridique lui donne vocation à collaborer à différents projets au sein d'EADS et des entités du Groupe telle qu'Airbus par exemple.

Titulaire d'un DEA en droit des contentieux public et privé, elle a débuté sa carrière en cabinet d'avocat, avant de se spécialiser sur les questions relatives au droit du numérique et des systèmes d'information.

Elle prépare actuellement, une thèse sur le cadre juridique des systèmes d'information embarqués, appliqué à l'aéronautique.

Son domaine d'expertise et ses travaux portent sur des thèmes comme la signature électronique, les logiciels libres, le droit de la cryptologie, l'identité électronique, la gestion des droits de propriété intellectuelle sur les logiciels, rédaction de rapports et d'études spécifiques, la négociation et la rédaction de contrats liés au numérique... Tout ceci dans un contexte aéronautique.





Martine RICOUART-MAILLET, avocat au Barreau de Lille

Spécialisation

Droit de la propriété intellectuelle : droit des marques, droit d'auteur, dessins & modèles, droit de la publicité et du multimédia, droit de la presse & de l'audiovisuel, droit de l'informatique, droit de l'Internet et du commerce électronique.

- Cofondatrice du cabinet BRM Avocats, 1988 ;
- Certificat de spécialisation en propriété intellectuelle et TIC ;
- Diplômée du Centre d'Études Internationales de la propriété industrielle de Strasbourg (C.E.I.P.I.) ;
- Cofondatrice du G.E.I.E. ARMODIOS : Réseau d'Avocats Européens spécialisés en PI, communication et médias ;
- Mandataire O.H.M.I. (Office européen des marques).



Enseignement

- Mastère Spécialisé Management et Protection des données à caractère personnel, Institut supérieur d'électronique de Paris Assas (ISEP) ;
- Master de communication internationale à l'I.A.E. de Lille ;
- IEP de Lille.

Associations

- Administrateur de l'AFCDP (Association française des Correspondants aux données personnelles) ;
- Membre de l'Association Internationale pour la Protection de la Propriété Intellectuelle (A.I.P.P.I.) ;
- Administrateur de l'association CYBERLEX (présidente 2003-2005) – <http://www.cyberlex.org>.

13,14 et 15 octobre 2009	Salon VAD e-commerce : « Outil de gestion de la relation client : Quelles précautions prendre au titre de la Loi Informatique & Libertés ? », « Opt-in partenaires : Etat des lieux », « Bases de données marketing : Aspects juridiques essentiels » « Flux transfrontières : Quel casse-tête ! »
29 août 2009	Maison des Associations de Lille, « Le droit de la presse est-il adapté aux nouveaux médias ? »
12 juin 2009	Institut supérieur d'électronique de Paris Assas (ISEP) - Mastère Spécialisé Management et Protection des données à caractère personnel, « Les acteurs de la cybersurveillance en entreprise : Quels droits ? Quelles obligations ? »
27 novembre 2008	Conférence Net 2008, « Technologies mobiles et législation informatique et libertés »
17 mars 2008	Cercle du marketing direct, « Nouveau cadre législatif de l'opt-in »

TAB. B.1 – Animatrice de séminaires et colloques



Raphaël Marichez, consultant en sécurité

Ingénieur de l'École polytechnique et de Télécom ParisTech (ENST Paris), Raphaël Marichez participe à plusieurs activités associatives, notamment l'association Polytechnique.org qu'il a présidée durant deux ans, et l'équipe sécurité de Gentoo Linux.

Après des stages en cryptographie et en conseil dans les technologies de l'information, il rejoint l'équipe HSC en 2006 avec une expertise dans les domaines du courrier électronique et de la lutte contre le spam.

Raphaël Marichez développe une compétence SSI mixte technique et organisationnelle depuis 2007, en étant successivement certifié ISO 27001 Lead Auditor, Lead Implementer, puis ISO 27005 IS Risk Manager par LSTI.

Il mène pour HSC des audits techniques ou organisationnels de sécurité, des études mixtes telles que des tests techniques adossés à des évaluations de conformité normative et des assistances à la mise en oeuvre de SMSI et d'appréciations des risques.

Il participe à la dispense des formations sur les normes ISO 27001/27005 comme sur les tests d'intrusions, et a créé la formation HSC "Juridique de la SSI".



Annexe C

Le point de vue de la Cnil

Copie-écran de la Fiche de synthèse « Les fichiers de journalisation », CYBER SURVEILLANCE SUR LES LIEUX DE TRAVAIL, 11 février 2002, p.4, accessible via le lien : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/cyber_fiches.pdf

Mention d'information : Il est précisé que la Cnil n'a pas participé, ni approuvé le contenu du présent livre blanc. La copie-écran afférente à la fiche de synthèse sur les fichiers de journalisation est insérée afin d'illustrer sa position sur les logs.



LA CYBERSURVEILLANCE SUR LES LIEUX DE TRAVAIL

*Conclusions du rapport présenté par M. Hubert BOUCHET,
vice-président délégué de la CNIL et adopté par la CNIL LE 5
février 2002*

Les fichiers de journalisation

Les fichiers de journalisation des connexions permettent d'identifier et d'enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations.

Il n'ont pas pour vocation première le contrôle des utilisateurs.

Ils ont pour finalité de garantir une utilisation normale des ressources des systèmes d'information mais ils peuvent être associés à des traitements d'information qui revêtent un caractère sensible pour l'entreprise ou l'administration concernée.

Ils constituent une mesure de sécurité généralement préconisée par la CNIL.

Les utilisateurs doivent être informés de la mise en place des systèmes de journalisation et de la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur sont conservées ou sauvegardées.

Cette information réalise l'obligation légale à laquelle est tenu le responsable du traitement, est de nature à prévenir tout risque et participe de l'exigence de loyauté dans l'entreprise ou l'administration. Une durée de conservation de l'ordre de 6 mois ne paraît pas excessive au regard de la finalité des fichiers de journalisation.

Aucune disposition de la loi du 6 janvier 1978 ne prive le responsable de l'entreprise de la possibilité d'opposer les informations enregistrées dans les fichiers de journalisation associés à un traitement automatisé d'informations nominatives à un salarié ou un agent public qui n'en n'aurait pas respecté les conditions d'accès ou d'usage (Cour de cassation – chambre sociale n° 98-43.485 du 18 juillet 2000).

En tant que tels, lorsqu'ils sont associés à un traitement automatisé d'informations nominative, ces fichiers de journalisation (proxis, caches, fire wall, ...) n'ont pas à faire l'objet de déclaration auprès de la CNIL.

La mise en œuvre d'un logiciel d'analyse des différents journaux (applicatifs et systèmes) permettant de collecter des informations individuelles poste par poste destiné à contrôler l'activité des utilisateurs, en revanche, doit être déclaré à la CNIL.

Annexe D

La politique type de gestion des journaux informatiques du Comité Réseau des Universités

La politique type de gestion des journaux informatiques du Comité Réseau des Universités version 2.6 novembre 2008, dont les copies-écran sont reproduites ci-dessous est accessible via le lien : http://www.cru.fr/activites/securite/index#gestion_des_traces.



Politique type de gestion des journaux informatiques

Version 2.6 novembre 2008

Ce document a été réalisé dans le cadre du groupe de travail SDS-SUP, mandaté par la Conférence des Présidents d'Université (CPU), la direction générale de la recherche et de l'innovation (DGRI), la direction générale de l'enseignement supérieur (DGES) et le Haut fonctionnaire de défense et de sécurité (HFDS) du ministère en charge de l'enseignement supérieur et la recherche.

La mission du groupe travail SDS-SUP animé par le CRU (Comité réseau des universités) est de mener des réflexions et de constituer un référentiel documentaire dans le domaine de la sécurité des systèmes d'information, notamment concernant les meilleures pratiques.

A ce titre, la « Politique type de gestion des journaux informatiques » s'est inspiré du document de « Politique de gestion de traces » du CNRS. Il a été mis à jour et complété afin garantir la cohérence globale des référentiels et la conformité à la législation et aux réglementations en vigueur, notamment pour les points relevant de la loi « informatique et libertés ». Le partenariat CPU/CNIL a permis de mener un travail collaboratif entre le groupe de travail SDS-SUP et la CNIL.

Dans un courrier du 26 novembre 2008 adressé à Mr Jean-Pierre Finance, président de la CPU, Mr Alex Turk, président de la CNIL nous fait part de quelques remarques intégralement prises en compte dans cette version du document.



Politique de gestion des journaux informatiques

à

1 Définitions

- on entend par « établissement » « (désignation du nom)..... » ;
- on entend par « utilisateur » les personnels, étudiants, stagiaires, personnes invitées et en règle générale toute personne utilisant les moyens du système d'information ;
- on entend par « entités » les composantes, services ou laboratoires...

2 Contexte

Le fonctionnement de l'établissement passe par l'utilisation de systèmes d'information et de moyens de communications qui s'appuient sur des réseaux télématiques connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une grande vulnérabilité intrinsèque, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que dans certaines situations celle de l'établissement qui met ces moyens à leur disposition en tant qu'outils de travail.

L'utilisation des nouvelles technologies de communication pose le problème de la protection d'une part de l'information sensible¹ gérée par les utilisateurs et d'autre part des systèmes d'information sous la responsabilité de l'établissement. Les mesures mises en œuvre doivent permettre à l'établissement de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, des réglementations sur la protection des données sensibles et la protection du patrimoine scientifique, de la loi sur la protection des données à caractère personnel (respect des droits de l'individu) et la sécurité des systèmes d'information.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des utilisateurs. L'établissement a mis en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens télématiques, et d'autre part a fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque utilisateur.

3 Principes de base

Une maîtrise de la fiabilité et de la sécurité du fonctionnement des systèmes d'information et une garantie de la légalité des transactions opérées nécessitent un contrôle s'appuyant nécessairement

¹ Informations sensibles au sens où la confidentialité (contrat, données de recherche, information nominatives, ...), l'intégrité (informations de gestion,...) et la disponibilité nécessitent une protection particulière.



sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque transaction, appelées journaux informatiques (ou logues).

3.1 Finalités des traitements

Les traitements de ces journaux informatiques ont pour finalités :

- de contrôler le volume d'utilisation de la ressource, détecter des anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins (métrologie) ;
- de vérifier que les règles en matière de sécurité des systèmes d'information (SSI) sont correctement appliquées ;
- de détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- de détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité de l'établissement ;
- de détecter les utilisations des moyens informatiques contraires aux chartes ou au règlement intérieur de l'établissement.
- d'être à même de fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition de l'autorité judiciaire présentée dans les formes légales.

Les finalités précitées imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient de remonter à l'utilisateur.

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 dite loi "Informatique et libertés". Ils doivent avoir satisfait au principe d'information préalable et de transparence ainsi qu'au régime déclaratif en vigueur auprès de la CNIL.²

3.2 Durée de conservation

La durée de conservation des journaux informatiques est de 1 an maximum. L'établissement s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme. Deux conteneurs de données sont donc définis, le premier reçoit les fichiers de logues vieux de moins de trois mois et les fichiers anonymisés quand ils existent. Le second reçoit les journaux contenant des données à caractère nominatif de plus de trois mois.

3.3 Qualités des données collectées

Les informations journalisées doivent être factuelles et contextuelles, c'est à dire qu'elles doivent permettre de connaître l'environnement de la collecte, le système hôte, les logiciels mis en œuvre etc. L'heure relevée est une information importante parce qu'elle est souvent le premier élément utilisé pour rapprocher des journaux de différents serveurs. Il est donc indispensable que les machines produisant des

² Voir la fiche pratique relative au contrôle de l'utilisation des moyens informatiques dans le *Guide pratique Informatique et Libertés pour l'enseignement supérieur et la recherche* (ce guide est disponible sur le site de la CNIL et celui de l'AMUE)



logues soient synchronisées sur un serveur de temps,

D'éventuelles interruptions de la journalisation doivent être repérables par les destinataires de ces données.

3.4 Sécurité et intégrité des données

La politique de sécurité du système d'information (PSSI) fixe les règles de sécurité appliquées à ces fichiers. Ces règles assurent l'intégrité des données en les protégeant en particulier contre un effacement ou des modifications malveillantes. Au besoin, une base d'empreintes numériques ou des jetons d'horodatage permettent de surveiller l'intégrité des fichiers de journaux.

Les règles de sécurité limitent l'accès aux fichiers de logues de moins de trois mois aux seuls administrateurs destinataires de ces données tel qu'ils sont définis au paragraphe 4.2.1 avec authentification préalable. Les accès sont ponctuels et motivés par les tâches de ces personnes. Le contenu de données consacré aux logues de plus de trois mois est en accès limité au RSSI et aux personnes désignées par le RSSI pour la mise en œuvre du droit d'accès aux intéressés et l'accès sur requête judiciaire.

La politique de sauvegarde de l'ensemble des données de l'établissement identifie les journaux contenant des données à caractère personnel dans le but de garantir leur suppression au delà d'une année.

Dans le cas d'une exploitation des journaux informatiques anonymisés, une copie anonymisée des logs est effectuée. L'anonymisation est réalisée dans le respect des règles de l'art, elle est irréversible. On se référera en particulier à l'expertise³ publiée par la CNIL dans ce domaine.

4 Les intervenants

4.1 Les utilisateurs

Tous les utilisateurs, tel qu'ils sont définis en introduction de ce document, sont tenus de respecter la politique de sécurité et les chartes en vigueur dans l'établissement.

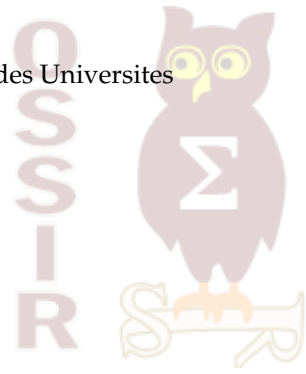
4.2 La chaîne fonctionnelle SSI

En dehors des acteurs de la chaîne fonctionnelle rappelée ci-dessous, personne n'a de droit d'accès aux journaux informatiques comportant des données à caractère personnel, y compris la chaîne hiérarchique. Ils sont tenus au devoir de réserve ou de discrétion professionnelle, voire au secret professionnel.

4.2.1 Les administrateurs systèmes et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et veillent au respect des règles de sécurité des systèmes d'information. À ce titre, ils gèrent les traces dans le respect des obligations générales de leur fonction (politique de sécurité, chartes).

³ <http://www.cnil.fr/index.php?id=1536>



Ils rapportent, à leur supérieur dans la chaîne fonctionnelle SSI, toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.

Ils acceptent d'exécuter des traitements ou de fournir des informations pouvant inclure des données à caractère personnel uniquement à la demande de la chaîne fonctionnelle de sécurité.

4.2.2 Les autres acteurs de la chaîne fonctionnelle SSI :

- les correspondants 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),
- le fonctionnaire de sécurité de défense (FSD).

Ils sont également tenus au devoir de discrétion professionnelle, et dans certains cas de secret professionnel en fonction de leur mission.

5 Les informations enregistrées

5.1 Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'augmentation de ses droits, tout ou partie des informations suivantes peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :

- l'identifiant de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- les commandes passées.

Le choix d'une politique de centralisation des journaux informatiques des postes de travail peut être fait.

5.2 Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs hébergeant ces services mis en œuvre au sein de l'établissement enregistrent pour chaque message émis ou reçu tout ou partie des informations suivantes :

- l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
- l'adresse des destinataires ;
- la date et l'heure de la tentative ;
- les différentes machines traversées par le message ;
- le traitement « accepté ou rejeté » du message ;
- La taille du message ;



- Certaines en-têtes du message, tel que l'identifiant numérique de message ;
- Le résultat du traitement des courriers non sollicités (spam) ;
- Le résultat du traitement antiviral ;
- Les opérations de validation ou de rejet par les modérateurs quand cela s'applique.

Les éléments de contenu des messages ne sont pas journalisés, néanmoins, les applications peuvent inclure des archives qui ne relèvent pas des journaux informatiques (chrono départ et réception).

5.3 Serveurs Web

On distingue les serveurs web exploités au sein de l'établissement et ceux situés en dehors de l'établissement

5.3.1 Serveurs Web de l'établissement

Pour chaque connexion les serveurs Web enregistrent tout ou partie des informations suivantes en fonction des exigences de qualité de service et de sécurité de l'application web :

- les noms ou adresses IP source et destination ;
- les différentes données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
- l'URL de la page consultée et les informations fournies par le client ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;
- les différents paramètres passés.

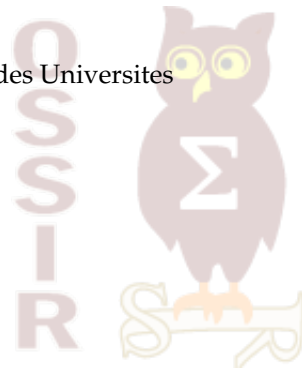
5.3.2 Serveurs Web hors établissement

Lors que les utilisateurs sont des membres de l'établissement, pour chaque accès web via le réseau interne vers des serveurs externes peuvent être enregistrées tout ou partie des informations suivantes :

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

L'article L.34-1 du code des postes et des communications électroniques précise que les opérateurs de communications électroniques sont tenus à une obligation de conservation des données de connexion mais que celles-ci "ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications". Cette interdiction s'applique donc en particulier à l'URL des pages consultées dans le cas où l'établissement offre des accès internet à des personnes extérieures à l'établissement. En effet, il est alors possible d'assimiler le service réseau de l'établissement à celui d'un opérateur de communications électroniques.

5.4 La téléphonie sur IP



L'usage de la téléphonie sur IP peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux, mais bien entendu, les principes relatifs à la loi « Informatique et Libertés » s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie.

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. Cependant, l'établissement peut éditer des relevés contenant l'intégralité des numéros appelés dans le cas où il demande aux personnels le remboursement du coût des communications personnelles ou dans celui où il a été constaté une utilisation manifestement anormale.

Le régime déclaratif de ces journaux fait l'objet de la norme simplifiée n° 47⁴ relative à l'utilisation de services de téléphonie fixe ou mobile sur les lieux de travail. En outre, la fiche pratique n°11 du guide « informatique et libertés » pour l'enseignement supérieur et la recherche⁵ intitulée « Utilisation du téléphone sur le lieu de travail » détaille ce cas.

5.5 Les équipements réseau

On appelle « équipements réseau » les routeurs, pare-feu, commutateurs, bornes d'accès, équipement de métrologie et d'administration de réseau, etc. Pour chaque paquet qui traverse l'équipement tout ou partie des informations suivantes peuvent être collectées :

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure de la tentative ;
- la façon dont le paquet a été traité par l'équipement ;
- le nombre de paquets et le nombre d'octets transférés ;
- ;
- les messages d'alerte.

5.6 Les applications spécifiques

On entend par « applications spécifiques », toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation.

Parmi ces applications nous pouvons citer les exemples suivants :

- accès aux bases de données ;
- accès à l'ENT (espace numérique de travail) ;
- service d'authentification (SSO, radius, ...) ;

Comme dans le cas des serveurs web internes, des journaux génériques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- l'identité de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative ;
- les volumes de données transférées ;

⁴ <http://www.cnil.fr/index.php?id=1777>

⁵ http://www.cnil.fr/fileadmin/documents/approfondir/dossier/education/Guide_InfoLib_Web.pdf



- les commandes passées ;

Le traitement des logues décrit ici ne couvre pas l'ensemble des données conservées par ces applications qui de par leur nature peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations ont un caractère personnel, elles sont alors soumises aux obligations de la loi Informatique et Libertés (déclaration auprès de la CNIL sauf en cas de désignation d'un Correspondant Informatique et Libertés (CIL), information préalable, etc).⁶

6 Finalités des traitements effectués et leurs destinataires

Les traitements effectués doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée.

6.1 Résultats statistiques

Ceux-ci sont effectués automatiquement et permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en temps qu'outil de travail. Lors de l'exploitation de ces résultats on s'attachera à distinguer les résultats anonymes de ceux qui peuvent être rapprochés de l'identité d'une personne. Parmi tous ces traitements on trouvera :

- des traitements statistiques en anonyme, en volume transféré et en nombre de connexions ;
- des classements des services les plus utilisés en volume de données et en nombre de connexions ;

Les résultats « anonymes » peuvent être conservés au-delà des délais mentionnés au paragraphe 3 et être diffusés sur des sites Internet accessibles à tous. Par contre, les administrateurs systèmes et réseau limitent l'accès aux résultats contenant des données à caractère personnel à eux-mêmes et éventuellement à la chaîne fonctionnelle SSI. La durée de conservation de ces statistiques non anonymisées ne peut excéder celle des journaux utilisés pour produire ces statistiques.

6.2 Résultats d'analyse

La politique de sécurité, applicable à chaque ressource informatique qui génère des traces, définit des règles d'analyse systématique de ces traces afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d'incident, des analyses peuvent être faites par les administrateurs systèmes et réseau sur les traces disponibles. Les résultats ne peuvent être transmis qu'à la chaîne fonctionnelle SSI et au CERT-Renater ou CERTA pour les incidents de sécurité.

Dans ce cas, l'accès aux trafics et aux traces est limité aux exploitants des systèmes en charge d'analyser l'incident et au RSSI. L'extraction de l'information et son utilisation sont strictement limitées à l'analyse de l'incident. Si l'incident n'est pas avéré les résultats sont non transmis et

⁶ Le Correspondant Informatique et Libertés a été introduit en 2004 avec la réforme de la loi informatique et libertés. Sa désignation permet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisations et continuent à faire l'objet de formalités. Il a un rôle de conseil et suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion de données à caractère personnel.



immédiatement détruits.

6.3 Détection des usages abusifs

On entend ici par « usages abusifs » les usages du réseau qui sont contraires aux lois, règlement intérieur ou chartes d'usage des moyens informatiques. Sont aussi visés les usages qui compromettent les services du réseau de l'établissement (consommation excessive de bande passante, introduction de faille dans la sécurité du réseau, etc).

Les logues peuvent être exploités pour mettre en évidence ces abus. Par exemple, des classements des machines ayant consommé le plus de réseau en volume transféré et en nombre de connexions permettent souvent de détecter l'utilisation indésirable de protocoles de peer to peer ou la présence de serveurs pirates. Se référer à la fiche pratique « Contrôle de l'utilisation des moyens informatiques » du *guide pratique « Informatique et Libertés » pour l'enseignement supérieur et la recherche*.

Quand ils sont mis en œuvre, ces traitements le sont de façon systématique (ils sont appliqués à toutes les machines du réseau de l'établissement ou d'une partie donnée du réseau) et ne ciblent aucune personne ou catégorie de personnes.

6.4 Des journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête. Dès l'apparition d'un incident, les journaux bruts pourront être requis par la chaîne fonctionnelle.

Les administrateurs systèmes et réseau sont chargés de l'application de la requête, et ils sont, pour cette activité, soumis au secret professionnel.

Les journaux bruts sont remis, à sa requête à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

6.5 Droit d'accès individuel

Chaque agent peut demander à consulter les traces qui le concernent. Les demandes doivent être faites par écrit auprès du directeur de l'entité d'hébergement. Conformément à l'article 39 de la loi « informatique et libertés » du 6 janvier 1978 modifiée et à l'article 92 décret du 20 octobre 2005 modifié en 2007, pris pour l'application de la loi précitée, les personnes souhaitant exercer leur droit d'accès doivent justifier de leur identité.

La recherche est faite par l'administrateur, sur demande de sa hiérarchie, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un «courrier personnel».

7 Informations des utilisateurs sur la politique de gestion des journaux informatiques

L'établissement doit informer ses utilisateurs de la gestion qui est faite des traces qui les concernent. Cela sera fait par la diffusion systématique de ce document qui sera référencé dans la charte informatique de l'établissement. Ce document sera rendu accessible à tout utilisateur par le réseau. Il pourra être mis en valeur dans l'intranet de l'établissement ou par voie d'affichage. Une attention particulière sera portée à la publicité de ce document lors de la mise à disposition de nouveaux services concernés par les journaux informatiques ainsi qu'auprès des nouveaux



utilisateurs des moyens informatiques de l'établissement.⁷

Une information et une consultation préalable des instances représentatives des personnels doit être prévue.

⁷ Se reporter au guide pratique de la CNIL à l'attention des employeurs, sections "cybersurveillance sur le lieu de travail", "le contrôle de l'usage de la messagerie électronique", "le rôle des administrateurs informatiques"