Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 2 décembre 2013

N° DAT-NT-012/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 24

Note technique

Recommandations de sécurité pour la mise en œuvre d'un système de journalisation

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurité pour la mise en œuvre d'un système de journalisation** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BSC, BAS, BAI, FRI, MRR	BSS	SDE	2 décembre 2013

Évolutions du document :

Version	Date	Nature des modifications
1.0	2 décembre 2013	Version initiale

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Introduction 4

2 Prérequis à la mise en place d'un système de journalisation 5

2.1 Fonctionnalité de journalisation . . . 5
2.2 Horodatage des évènements . . . 5
2.3 Synchronisation des horloges . . . 5
2.4 Dimensionnement . . . 6
2.4.1 Espace disque . . . 6
2.4.2 Résistance à la charge . . . 7

3 Recommandations d'architecture et de conception 8

3.1 Résilience du système de journalisation . . . 8
3.1.1 Exportation des journaux . . . 8
3.1.2 Centralisation des journaux . . . 8
3.2 Protection des données échangées . . . 9
3.2.1 Modes de transfert . . . 9
3.2.2 Prétraitement des journaux . . . 10
3.2.3 Fiabilisation du transfert des journaux . . . 10
3.2.4 Sécurisation du transfert des journaux . . . 10
3.2.5 Bande passante . . . 11
3.2.6 Utilisation du réseau d'administration . . . 11
3.3 Stockage . . . 11
3.3.1 Partition séparée . . . 11
3.3.2 Arborescence . . . 12
3.3.3 Rotation . . . 12
3.3.4 Archivage . . . 12
3.3.5 Protection des journaux . . . 13
3.4 Consultation . . . 13
3.4.1 Choix d'un outil . . . 13
3.4.2 Définition des rôles . . . 14
3.5 Supervision de l'espace disque . . . 14

Annexes 15

A Choix des évènements 15

B Illustrations 16

B.1 Architecture de journalisation simple . . . 16
B.2 Architecture de journalisation étendue/multi-sites . . . 17

C Aspects juridiques et réglementaires 18

C.1 Valeur probatoire des éléments de journalisation . . . 18
C.2 Régime général de protection des données à caractère personnel . . . 18

C.3 Régimes particuliers relatifs à la conservation des éléments de journalisation 19
C.3.1 Conservation des éléments de journalisation par les fournisseurs d'accès à Internet (FAI) ou d'hébergement 19
C.3.2 Conservation des éléments de journalisation des opérateurs de communications électroniques 20
C.3.3 Accès aux éléments de journalisation par les autorités judiciaires 20
C.4 Surveillance des salariés 20
C.5 Réglementations sectorielles 21
C.6 Récapitulatif 22

1 Introduction

Les journaux d'évènements constituent une brique technique indispensable à la gestion de la sécurité des systèmes d'information, quelles que soient la nature et la taille de ces derniers. Les journaux sont une source d'information riche qui peut être utilisée *a priori* pour détecter des incidents de sécurité. Dans ce cas, les évènements constituant les journaux sont consultés et analysés en temps réel. Les journaux peuvent également être employés *a posteriori* pour retrouver les traces d'un incident de sécurité ; l'analyse des journaux d'un ensemble de composants (postes de travail, équipements réseaux, serveurs, etc.) peut alors permettre de comprendre le cheminement d'une attaque et d'évaluer son impact. Il faut donc garder à l'esprit que l'activité de journalisation est un moyen de détection et d'analyse. Elle ne se substitue pas aux mécanismes de protection du système d'information, elle doit être employée de façon complémentaire. L'utilité des journaux d'évènements dépend de leur génération et de leur récupération, une architecture de journalisation doit donc suivre l'évolution du système d'information concerné (prise en compte des nouveaux équipements, des nouveaux usages, etc.).

Ce document a pour objectifs, d'une part, de détailler les prérequis nécessaires à la mise en œuvre d'un système de journalisation efficace et sécurisé et, d'autre part, de présenter les bonnes pratiques permettant de bâtir une architecture de gestion de journaux pérenne, quelle que soit la nature du système d'information. La granularité des mesures présentées dans ce document doit être adaptées aux résultats d'une analyse de risques menée en amont. Ce document n'a pas vocation à présenter la liste détaillée des évènements à journaliser, ceux-ci étant dépendants des systèmes et des applicatifs employés. Il peut faciliter la formalisation des règles et métriques sous la forme d'une politique de journalisation.

Les aspects légaux et réglementaires relatifs à la journalisation des évènements sont également abordés dans les annexes de ce document.

2 Prérequis à la mise en place d'un système de journalisation

2.1 Fonctionnalité de journalisation

Si les systèmes d'exploitation modernes incluent en général nativement des fonctionnalités de journalisation, cela n'est pas forcément le cas pour des applicatifs tiers développés pour des besoins métiers spécifiques. C'est la raison pour laquelle la fonctionnalité de journalisation doit être prise en compte dans les cahiers des charges fonctionnels et techniques au lancement d'un projet, quelle qu'en soit sa nature. Il doit ainsi être possible d'enregistrer des évènements liés à la sécurité (par exemple l'authentification des utilisateurs) ainsi qu'à l'activité correspondant au service fourni par l'applicatif (par exemple l'accès à une ressource).

Les journaux doivent si possible être générés dans un format interprétable, c'est-à-dire compréhensible à la lecture et facilement analysable de manière automatique par des outils informatiques. Les évènements inscrits dans les journaux doivent être composés de champs fixes à la grammaire bien définie, celle-ci pouvant évoluer en fonction des versions des systèmes qui génèrent les journaux. Un évènement doit contenir en particulier une source identifiable (un équipement, un utilisateur, un nom de processus ou plusieurs de ces éléments) permettant de déterminer avec le plus de précision possible son origine. L'absence de journaux rendra difficile, voire impossible, la détection d'incidents de sécurité, le reporting, le diagnostic en cas de problème et pourra constituer une infraction (se reporter à l'annexe C). La présence et l'exploitation des journaux contribue au maintien en conditions de sécurité de l'ensemble des briques qui constituent un système d'information.

R1	Utiliser des systèmes et des applicatifs disposant nativement d'une fonctionnalité de journalisation est primordial. La prise en compte de cette fonction doit se faire lors de toute démarche de conception et de développement.

2.2 Horodatage des évènements

Un évènement journalisé n'est pertinent que si celui-ci peut être situé dans le temps, et ce pour plusieurs raisons :

- la signification de cent occurrences d'un même évènement n'est pas la même selon qu'elles ont lieu durant un laps de temps d'une journée ou de dix minutes. Dans le premier cas, il peut s'agir par exemple d'un fonctionnement normal, alors que dans le second, cela peut être caractéristique d'un incident de sécurité. La fréquence d'occurrence d'un évènement peut donc être un élément essentiel pour détecter un incident de sécurité et apprécier sa gravité ;
- la détection d'un incident ou sa compréhension *post-mortem* nécessite généralement le croisement de journaux issus de différents équipements. L'absence d'horodatage homogène des évènements rendra très difficile le recoupement des informations (se référer au paragraphe 2.3) ;
- l'horodatage d'un évènement peut aider à déterminer la nature de celui-ci. Par exemple, s'il se produit à intervalles réguliers (toutes les heures à la seconde près par exemple), il est probable qu'il soit le résultat d'une opération automatique et non manuelle.

R2	L'horodatage doit être activé pour l'ensemble des évènements afin de permettre une meilleure exploitation des journaux.

2.3 Synchronisation des horloges

L'ensemble des équipements informatiques dispose normalement d'une horloge interne utilisée entre autres pour horodater les journaux d'évènements. Cependant, les horloges de tous les équipements

dérivent naturellement dans le temps. Si les écarts peuvent paraître minimes de prime abord, ils peuvent se mesurer en secondes voire en minutes après quelques semaines.

Il est donc crucial de disposer d'équipements synchronisés sur la même base de temps pour pouvoir analyser convenablement les journaux collectés. La compréhension de l'enchaînement précis d'évènements issus de plusieurs types de journaux est beaucoup plus difficile si les équipements qui produisent ces journaux ne disposent pas du même temps de référence. Un laps de temps très court (quelques secondes) peut séparer deux évènements caractérisant un incident de sécurité. Si un décalage d'horloge existe entre les machines qui ont généré ces deux évènements, ils ne seront pas horodatés correctement et l'incident de sécurité pourrait ne pas être détecté.

Il est donc recommandé de mettre en œuvre une architecture permettant de disposer de sources de temps fiables utilisées par l'ensemble des équipements qui composent le système d'information. Plusieurs solutions peuvent être employées pour obtenir une source de temps précise. Il existe par exemple des serveurs de temps reconnus accessibles publiquement sur Internet, mais il est préférable d'utiliser une source de temps basée sur des signaux radio ou satellitaires. Il est également possible d'installer une source de temps autonome très stable (horloge atomique) pour ne pas dépendre de signaux extérieurs potentiellement sujets à des perturbations (volontaires ou non). Dans le cas des réseaux non-interconnectés, il n'est pas dans la plupart des cas nécessaire, ni même recommandé, de disposer de serveurs de temps synchronisés sur des sources externes ; en revanche, il est indispensable que les équipements soient synchronisés sur les mêmes sources de temps internes cohérentes entre elles.

Le protocole NTP (Network Time Protocol) est largement utilisé pour synchroniser les équipements sur une ou plusieurs sources de temps. Il est disponible pour la plupart des systèmes d'exploitation, quel que soit le type d'équipement. Une architecture NTP type comprend généralement un ou plusieurs serveurs NTP internes sur lesquels se synchronisent l'ensemble des machines du système d'information ; ces serveurs référents étant, quant à eux, synchronisés sur plusieurs sources (autonomes, serveurs NTP publics, signaux radio/satellitaires).

R3	Les horloges des équipements doivent être synchronisées sur plusieurs sources de temps internes cohérentes entre elles. Ces sources pourront elles-mêmes être synchronisées sur plusieurs sources fiables externes, sauf pour les réseaux isolés.

Lorsque les équipements sont répartis géographiquement sur des fuseaux horaires différents, il est important d'adopter une logique de configuration adéquate afin d'assurer une cohérence temporelle des journaux au niveau des serveurs de collecte. Dans certains cas, le choix d'un même fuseau horaire (heure UTC par exemple) sur l'ensemble des équipements peut être nécessaire.

2.4 Dimensionnement

2.4.1 Espace disque

Les journaux sont généralement stockés localement sous forme de texte compressé mais ils peuvent vite représenter des quantités de données importantes et provoquer une saturation de l'espace de stockage des équipements. Il est ainsi recommandé de prendre en compte les besoins d'espace disque nécessaires au stockage des journaux lors du dimensionnement des équipements. Les sections suivantes abordent la rotation des journaux et la mise en place de mécanismes d'exportation, ces mesures peuvent contribuer à la mise en œuvre de cette recommandation.

R4	Lors du dimensionnement des équipements, l'estimation de l'espace de stockage nécessaire à la conservation locale des journaux est indispensable.

2.4.2 Résistance à la charge

Quel que soit le composant qui génère des journaux (système d'exploitation, applicatif, etc.) il est important de connaître son comportement vis-à-vis de l'activité de journalisation en cas de charge anormale prolongée. Si le composant estime que les ressources disponibles sont insuffisantes, il est probable qu'il privilégiera ses fonctions principales au détriment des services secondaires comme la journalisation. La connaissance de ce comportement permet de dimensionner le composant en fonction des exigences relatives à son contexte d'usage.
La résistance à la charge dépend également des types d'évènements que l'on aura choisis de journaliser au niveau du composant (se reporter à l'annexe A).

3 Recommandations d'architecture et de conception

3.1 Résilience du système de journalisation

3.1.1 Exportation des journaux

L'exportation des journaux consiste à copier les évènements sur une machine différente de celle qui les a générés.

Cette mesure est nécessaire pour plusieurs raisons :

- les équipements qui génèrent les journaux peuvent ne pas disposer de l'espace disque nécessaire pour stocker une quantité de journaux suffisante au regard des contraintes métiers, légales ou réglementaires (se reporter à l'annexe C). La copie des journaux doit donc être réalisée sur des équipements tiers correctement dimensionnés ;
- si l'analyse des journaux a lieu dans le cadre d'investigations faisant suite à un incident de sécurité, il est possible que les journaux ne soient plus présents sur la machine source (effacement volontaire par un attaquant, défaillance matérielle, etc.). L'exportation permet de disposer d'une copie sur des équipements physiquement distincts.

R5	Les journaux doivent être automatiquement exportés sur une machine physique différente de celle qui les a générés.

3.1.2 Centralisation des journaux

La centralisation des journaux a pour but de faciliter leur exploitation. Ce mode de fonctionnement comporte plusieurs avantages :

- la consultation des journaux est simplifiée : les personnes en charge de l'exploitation n'ont pas à se connecter sur plusieurs équipements pour rechercher de l'information ;
- le recoupement d'informations provenant de journaux d'équipements différents est plus aisé lorsque ceux-ci sont stockés au même endroit ;
- la sauvegarde des journaux est facilitée.

R6	Les journaux de l'ensemble des équipements du système d'information doivent être transférés sur un ou plusieurs serveurs centraux dédiés.

Si la taille du système d'information est très importante (plusieurs milliers d'équipements) ou si celui-ci est composé de nombreuses entités (sites physiques, entités fonctionnelles), il est nécessaire d'assurer la résilience du serveur central sur lequel tous les journaux sont collectés. En effet, une indisponibilité même de courte durée peut entraîner la perte de journaux.

R7	Si le parc d'équipements qui génère des journaux est important, le serveur central devra être redondé afin d'accroître la disponibilité du service de collecte de journaux.

Dans certains cas, il peut être pertinent d'adopter une organisation hiérarchique. Des serveurs locaux collectent les journaux des équipements correspondant à leur périmètre physique ou fonctionnel puis ils les transmettent aux serveurs centraux qui ont la charge d'agréger la totalité des journaux du système d'information ou d'un sous-ensemble spécifique (base de données, système, etc.). Ils dupliquent également les journaux qu'ils conservent localement afin d'éviter les pertes en cas de dysfonctionnement lors du transfert au niveau supérieur. Une organisation de ce type comporte plusieurs avantages :

- la résilience de l'architecture de journalisation est meilleure : les serveurs de journalisation locaux peuvent pallier une indisponibilité des serveurs centraux. La copie des journaux conservée sur ces serveurs intermédiaires pourra être transmise au niveau central une fois la communication

rétablie. Cela nécessite la configuration d'une politique de rétention adéquate, c'est-à-dire adaptée à la volumétrie et aux exigences de disponibilité des serveurs centraux ;
- le nombre de flux réseau de journalisation est réduit : cela peut contribuer à un meilleur contrôle des matrices de flux des équipements de filtrage réseau ;
- les serveurs locaux peuvent apporter des fonctionnalités additionnelles dans la transmission des journaux (comme la compression ou le chiffrement), ce qui est particulièrement utile si des liens de faible capacité ou non sûrs sont utilisés pour véhiculer les journaux jusqu'aux serveurs centraux.

R8	Si la taille ou la typologie du système d'information le nécessite, une approche hiérarchique pour l'organisation des serveurs de collecte doit être retenue.

3.2 Protection des données échangées

3.2.1 Modes de transfert

En premier lieu, il convient de s'intéresser aux différents modes de transfert de journaux sur les équipements centraux, chacun ayant des avantages et des inconvénients.

Transfert en temps réel

Ce mode consiste à transférer les journaux sur les serveurs centraux au moment où ils sont produits, une copie étant généralement conservée localement par l'équipement qui génère les évènements. Ce mode présente l'avantage de rendre les journaux rapidement disponibles en consultation sur les serveurs centraux mais peut poser des problèmes réseau. En effet, l'envoi de journaux peut consommer une bande passante très importante et perturber les autres services (flux d'administration ou de supervision par exemple) même si ces données transitent sur un réseau dédié à l'administration (se référer au paragraphe 3.2.5).

Le mode de transfert en temps réel est celui qu'il est préférable de mettre en place dans la mesure où les journaux sont immédiatement disponibles sur les serveurs centraux, mais il ne doit être mis en œuvre qu'après une évaluation de son impact sur la bande passante.

Transfert en temps différé

Ce mode consiste à transférer périodiquement les journaux sur les serveurs centraux (tous les jours par exemple). Il présente l'avantage de ne pas consommer de façon permanente de la bande passante. Par exemple, le transfert de l'ensemble des journaux peut être réalisé en dehors des horaires métier afin d'éviter d'influer sur les autres services au niveau du réseau. Ce mode présente cependant l'inconvénient de retarder la mise à disposition des journaux en consultation au niveau central. Il est également plus risqué dans la mesure où si un incident de sécurité se produit entre deux envois de journaux, il ne pourra pas forcément être détecté (par exemple si un attaquant efface ou modifie volontairement les journaux pour masquer son activité).

Le mode de transfert en temps différé n'est donc pas recommandé. Il pourra toutefois être mise en œuvre si des contraintes liées à l'architecture ou au métier l'imposent.

R9	Si le contexte le permet, un transfert en temps réel des journaux sur les serveurs centraux doit être privilégié.

Quel que soit le mode de transfert utilisé, l'envoi des journaux peut être provoqué soit par l'équipement qui les génère (mode *push*), soit par le serveur de collecte (mode *pull*). Le mode *pull* présente l'avantage

de garder la maîtrise échanges, le serveur de journalisation étant plus de confiance que les équipements vers lesquels il établit les connexions pour récupérer les journaux. Cependant ce mode de fonctionnement peut présenter des risques importants si le serveur central est compromis, l'attaquant peut être en mesure d'atteindre l'ensemble des machines du système d'information. Il est donc indispensable de sécuriser le serveur de journalisation et de le placer dans une zone de confiance afin de minimiser les risques d'attaque par rebond. Dans certains cas, le mode *push* pourra être retenu si l'ensemble des équipements générant des journaux ne possèdent pas le même niveau de sensibilité, le serveur central devant être protégé au plus haut niveau.

3.2.2 Prétraitement des journaux

Il est déconseillé de modifier le format des journaux sur les machines émettrices avant leur envoi sur les serveurs centraux. Si l'objectif du traitement en amont est de faciliter le transfert des journaux en unifiant au plus tôt leur mise en forme, cela peut conduire à dénaturer les évènements et induire des pertes d'information. Les actions de conversion doivent être réalisées de préférence à l'aide d'outils installés sur les serveurs centraux, une copie non altérée des journaux y étant conservée pour archivage.

R10	Il est recommandé de ne pas effectuer de traitement sur les journaux avant leur transfert.

3.2.3 Fiabilisation du transfert des journaux

Les applications de transfert de journaux reposent sur les protocoles TCP ou UDP pour acheminer les données aux équipements centraux. Le plus simple des deux, le protocole UDP, présente l'avantage de prendre le minimum de ressources mais, il a l'inconvénient d'être peu fiable car sujet aux pertes de paquets. Le protocole TCP, quant à lui, améliore la fiabilité du transfert des journaux en ajoutant des fonctions de ré-émission de paquets, de mise en cache du côté de l'émetteur et d'acquittement envoyés par le destinataire. Il est donc à privilégier par rapport au protocole UDP.

R11	Il est recommandé d'utiliser des protocoles d'envoi de journaux basés sur TCP pour fiabiliser le transfert de données entre les machines émettrices et les serveurs centraux.

Cependant, l'usage du protocole TCP ne suffit pas à lui seul à garantir l'absence de perte de données. D'autres mécanismes présents au niveau applicatif permettent d'améliorer encore la fiabilité du transfert en ajoutant des fonctionnalités de cache et d'acquittement plus efficaces.

3.2.4 Sécurisation du transfert des journaux

Il est nécessaire de mettre en place des mécanismes de protection garantissant la confidentialité et surtout l'intégrité des flux de transfert des journaux, en particulier lorsque les données transitent sur des réseaux non maitrîsés. Le besoin en confidentialité est aussi fonction de la sensibilité des informations journalisées. L'idéal est de mettre en place un canal de transmission dédié réalisé à l'aide de mécanismes cryptographiques robustes [1]. Idéalement, ce canal doit être établi après authentification mutuelle de la machine émettrice et le serveur de collecte en utilisant des certificats issus d'une autorité de certification de confiance. Il existe pour certains protocoles de transfert de journaux une version sécurisée basée sur TLS qui permet de répondre à ces exigences.

R12	Il est recommandé d'utiliser des protocoles de transfert de journaux qui s'appuient sur des mécanismes cryptographiques robustes en particulier lorsque les données transitent sur des réseaux non maîtrisés.

1. Se référer à l'annexe B1 du Référentiel Général de Sécurité (RGS) disponible sur le site de l'ANSSI.

Si le protocole de transfert de journaux ne dispose pas nativement de mécanismes de chiffrement ou de signature, il est tentant de s'appuyer sur des solutions tierces telles que SSH [2] ou IPsec [3]. Cependant, le besoin essentiel du service de journalisation reste la disponibilité ; la complexité de mise en œuvre des mécanismes de sécurisation tiers ou leur manque de fiabilité dans le temps [4] ne doit pas nuire à ce critère.

3.2.5 Bande passante

Quel que soit la mode de transfert utilisé pour acheminer les journaux des machines sources sur les serveurs centraux (temps réel ou temps différé), l'activation des mécanismes de limitation de bande passante et/ou de priorisation des flux permet de garder la maîtrise de l'usage des ressources réseau, et ce même si l'envoi des journaux a lieu en dehors des horaires métier (en temps différé).

R13	Il est recommandé de bien contrôler la bande passante des flux réseau utilisée pour transférer les journaux d'évènements.

3.2.6 Utilisation du réseau d'administration

L'utilisation d'un réseau d'administration dédié et physiquement distinct de celui employé pour les échanges de données « métiers » est une bonne pratique d'ordre général qui doit être privilégiée. Lorsqu'il existe, il doit être utilisé en priorité pour faire transiter les journaux émis par les équipements administrés. Cette solution met à disposition de fait une bande passante plus importante sans affecter la disponibilité des services « métiers » et peut, lorsque la sensibilité des informations transmises le justifie, apporter une protection supplémentaire.

R14	Lorsque le besoin de sécurité pour le transfert des journaux est important, il doit se faire sur un réseau d'administration dédié.

Les réseaux d'administration doivent également être utilisés pour accueillir la zone réservée à l'hébergement des serveurs de collecte. En effet, ces derniers concentrent une quantité importante d'informations dont certaines sont sensibles, leur protection doit donc être assurée.

R15	S'il n'existe pas de réseaux d'administration dans l'architecture pour accueillir les serveurs de journalisation, ils doivent être placés dans une zone interne non exposée directement à des réseaux qui ne sont pas de confiance (par exemple Internet).

3.3 Stockage

Les recommandations qui suivent sont applicables à l'ensemble des équipements qui composent l'architecture de journalisation : équipements source, serveurs de journalisation locaux et centraux.

3.3.1 Partition séparée

Afin d'éviter la saturation des disques des équipements qui produisent ou centralisent des journaux, il est recommandé de créer une partition dédiée aux journaux d'évènements et disposant de droits d'accès restreints. Cette mesure permet d'éviter la défaillance du système ou de certains services qui n'auraient pas d'espace disque suffisant pour fonctionner correctement. Cependant des journaux

2. Se référer au guide « Recommandations pour un usage sécurisé d'OpenSSH » disponible sur le site de l'ANSSI.
3. Se référer au guide « Recommandations de sécurité relatives à IPsec pour la protection des flux réseau » disponible sur le site de l'ANSSI.
4. Gestion non rigoureuse du renouvellement des clés, péremption des certificats, etc.

pourraient être perdus si la partition dédiée venait à être saturée à son tour. C'est la raison pour laquelle une politique de rotation adéquate des journaux doit être mise en œuvre en complément de cette mesure (se référer au paragraphe 3.3.3).

R16	Une partition disque doit être dédiée au stockage des journaux d'évènements sur les équipements qui les génèrent ou qui les centralisent.

3.3.2 Arborescence

Un équipement, en fonction de son rôle, peut être amené à stocker différents types d'évènements (système, applicatif, etc.). Il peut être utile de stocker les journaux sous forme d'arborescence définie à l'aide de thématiques : authentification, applicatifs métiers, web, etc. Cela pourra faciliter le transfert massif des journaux, l'envoi d'un seul répertoire (généralement compressé) contiendra l'ensemble des journaux de l'équipement.

R17	Il est recommandé d'adopter une arborescence pour le stockage des journaux d'évènements.

3.3.3 Rotation

La mise en œuvre d'une politique de rotation des journaux consiste à configurer des mécanismes de traitement automatique qui permettent de conserver l'exploitabilité des journaux dans la durée tout en limitant l'espace disque utilisé. Le déclenchement de la rotation des fichiers de journaux peut être basé sur des contraintes temporelles (rotation tous les jours à minuit), ou de taille (rotation si le fichier de journal atteint 100 Mo). Le choix dépend des exigences et des contraintes spécifiques au système d'information.

Voici les traitements qui peuvent être réalisés lors de la rotation des journaux :

- séparation des fichiers : un nouveau fichier est créé au moment de la rotation pour éviter que les évènements soient stockés dans un seul fichier de taille trop importante. Les fichiers ainsi générés sont généralement nommés selon un format qui inclut la date et l'heure de création ainsi que le type de journal ;
- compression : les fichiers créés au moment de la rotation sont habituellement compressés afin de réduire leur occupation sur le disque ;
- effacement : pour éviter la saturation de l'espace disque local, les fichiers de journaux les plus anciens peuvent être effacés automatiquement lors de la rotation. Il convient de s'assurer que les journaux détruits ont été correctement exportés au préalable. Une durée de rétention adéquate doit donc être définie, elle sera fonction de l'espace disque disponible ainsi que des contraintes éventuelles d'exploitation. Dans le cas des serveurs centraux, cette durée doit être supérieure à l'écart qui sépare deux sauvegardes. Dans les autres cas (équipements source et serveurs de collecte locaux), cette durée doit être supérieure à l'écart qui sépare deux envois de journaux si le mode de transfert en temps différé est employé.

R18	Une politique de rotation des journaux d'évènements doit être formalisée et mise en œuvre sur l'ensemble des équipements du système de journalisation.

3.3.4 Archivage

L'archivage des journaux consiste à conserver les fichiers pendant une longue durée. Il est généralement réalisé sur des supports amovibles de grande capacité conservés hors ligne. Si la centralisation des journaux est correctement mise en œuvre, l'archivage est réalisé à partir des fichiers stockés sur les

serveurs de journaux centraux.

L'archivage des journaux est nécessaire pour plusieurs raisons :
- pour des questions fonctionnelles : si un incident de sécurité est avéré, la recherche d'informations dans des journaux même très anciens peut aider à en déterminer l'origine ou à en apprécier l'ensemble de ses impacts ;
- pour des questions d'ordre légal et réglementaire : la durée de conservation des fichiers de journaux est fixée par le cadre légal. D'autres contraintes réglementaires spécifiques peuvent s'appliquer en fonction du contexte métier, charge au lecteur de se renseigner auprès d'un organisme juridique afin de déterminer celles qui sont applicables au sien. L'annexe C aborde les contraintes légales et réglementaires relatives à la journalisation.

R19	La durée de conservation des fichiers de journaux étant soumise à des contraintes légales et réglementaires, il convient d'en prendre connaissance pour définir les moyens techniques nécessaire à l'archivage des journaux.

3.3.5 Protection des journaux

Droit d'accès

Les fichiers de journaux doivent être accessibles en écriture uniquement à partir de comptes disposant des privilèges de journalisation adéquats. Les droits d'accès en lecture dépendent du contexte. Dans certains cas, les utilisateurs peuvent ne pas être autorisés à consulter les journaux résultant de leur propre activité.

R20	L'accès aux journaux doit être limité en écriture à un nombre restreint de comptes ayant le besoin d'en connaître.

R21	Les processus de journalisation et de collecte doivent être exécutés par des comptes disposant de peu privilèges.

Fonctions de sécurité avancées

Dans des contextes métier spécifiques soumis à des contraintes réglementaires fortes, par exemple les jeux en ligne (se reporter à l'annexe C.5), certains types de fichiers de journaux doivent être protégés à l'aide de mécanismes cryptographiques robustes afin d'assurer leur intégrité, leur confidentialité et de renforcer leur valeur probatoire [5].

3.4 Consultation

3.4.1 Choix d'un outil

Les journaux stockés de façon centralisée doivent être facilement consultables à l'aide d'un outil adapté. Dans certains cas d'usage, il est nécessaire de retrouver rapidement les informations recherchées dans les journaux. L'outil utilisé doit donc être réactif et facile à utiliser. Les besoins fonctionnels sont le principal critère de sélection de l'applicatif employé pour exploiter les journaux, des contraintes technologiques peuvent également intervenir dans le choix de l'outil (type de stockage, format des

5. La liste des produits qualifiés répondant à ces besoins sont disponibles sur le site de l'ANSSI.

journaux, etc.).

R22	Un outil spécifique doit être utilisé pour une meilleure exploitation des journaux présents sur les serveurs centraux, la détection d'évènements anormaux en sera facilitée.

Les accès à l'outil de consultation des journaux doivent être journalisés au même titre que pour n'importe quel autre service.

3.4.2 Définition des rôles

En fonction du contexte, plusieurs types de populations peuvent accéder à l'outil mis à disposition sur les serveurs centraux pour exploiter les journaux. Ces groupes d'utilisateurs n'ont pas nécessairement besoin de disposer d'un accès en lecture à l'ensemble des journaux du système d'information (niveaux de sensibilité différents), c'est la raison pour laquelle il est recommandé de pratiquer un cloisonnement en définissant des rôles précis au niveau de l'outil de consultation des journaux. Ces rôles peuvent être calqués sur des entités métier qui ont besoin de consulter les journaux relatifs à leur activité (administrateurs systèmes, administrateurs de bases de données, administrateurs de sécurité, etc.). L'usage d'un annuaire préexistant est recommandé pour authentifier les utilisateurs de l'outil de consultation des journaux ; les groupes d'utilisateurs qu'il contient pourront alors être utilisés comme références pour définir ceux présents dans l'outil.

R23	Les comptes ayant accès à l'outil de consultation centralisée des journaux doivent être associés à des rôles prédéterminés.

3.5 Supervision de l'espace disque

Il est recommandé de superviser l'espace disque restant sur les espaces de stockage locaux des équipements qui génèrent et stockent les journaux, et ce, pour plusieurs raisons :

- de nombreux incidents de sécurité entraînant l'indisponibilité de services ont pour origine une saturation de l'espace de stockage local par les journaux ;
- si l'espace disque est saturé, des journaux pourraient être perdus si aucune politique de rotation n'est mise en œuvre ;
- une activité de journalisation anormale peut être détectée. Si un équipement journalise dans des proportions inhabituelles par rapport à une activité normale ou s'il ne journalise pas du tout, il est possible qu'un incident de sécurité soit en cours sur la machine ;
- l'ajout de nouveaux équipements dans le système d'information induit l'envoi de nouveaux journaux, il est important d'anticiper les besoins en espace disque des équipements centraux.

R24	L'espace disque des équipements qui génèrent et stockent les journaux doit être surpervisé.

La mise en place de seuils d'alerte (pourcentage d'espace disque restant) permet d'anticiper une saturation de l'espace de stockage des équipements.

Annexes

A Choix des évènements

Il est important de procéder à la sélection des évènements journalisés par les différents composants du système d'information. Journaliser la totalité des évènements peut entraîner une consommation excessive des ressources (processeur, mémoire, stockage, bande passante, etc.) et engendrer une quantité de données difficilement exploitable. À l'inverse, une politique de journalisation trop ciblée ne produira pas suffisamment de données utiles.

Ce paragraphe présente les principales thématiques d'évènements qu'il est recommandé de journaliser. Cette liste de haut niveau n'est pas exhaustive, elle peut être enrichie en fonction des exigences propres au contexte.

Thème	Exemple
Authentification	- réussites et échecs d'authentification - utilisations des différents mécanismes d'authentification - élévations de privilèges
Gestion des comptes et des droits	- ajouts/suppressions de comptes/groupes/rôles - affectations/suppressions de droits aux comptes/groupes/rôles - modifications des données d'authentification
Accès aux ressources	- accès ou tentatives d'accès en lecture/écriture/exécution aux ressources
Modification des stratégies de sécurité	- éditions, applications, réinitialisations de configurations
Activité des processus	- démarrages/arrêts - dysfonctionnements - chargements/déchargements de modules
Activité des systèmes	- démarrages/arrêts - dysfonctionnements/surcharges du système - chargements/déchargements de modules - activité matérielle (défaillances, connexions/déconnexions physiques, etc.)

D'autres éléments caractérisant les évènements doivent également être pris en compte lors de la configuration des paramètres de journalisation : niveau de sévérité, niveau de verbosité, fréquence d'émission, etc.

B Illustrations

Les figures présentées dans ce paragraphe ont simplement pour objectif d'illustrer deux types d'architectures de journalisation centralisées. La première représentant un système d'information de dimension réduite, la seconde un système plus étendu ou multi-sites.

B.1 Architecture de journalisation simple

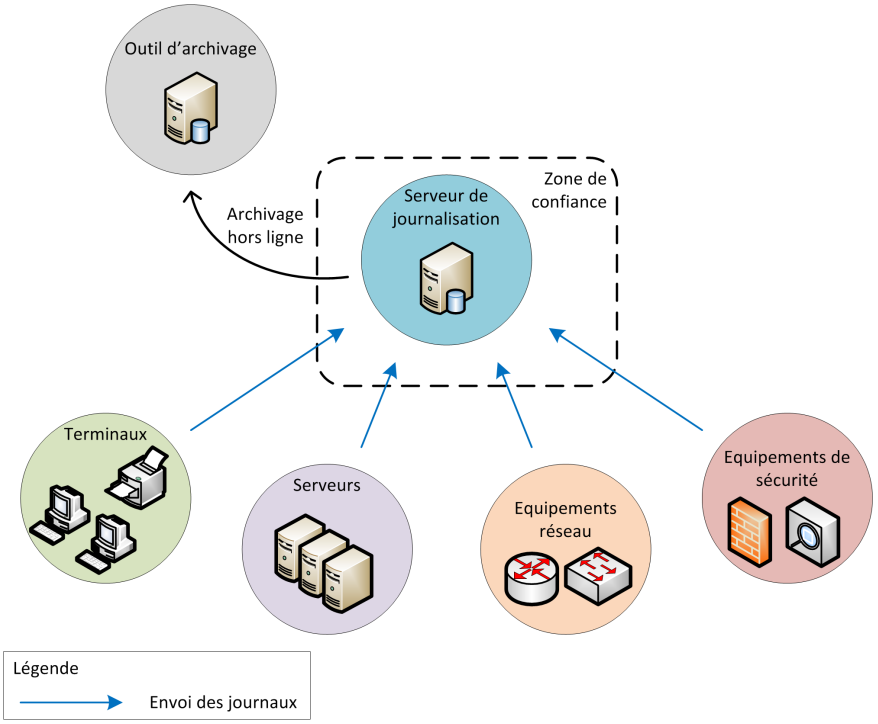

FIGURE 1 – Exemple d'architecture de journalisation simple

Cette architecture minimaliste ne comporte qu'un seul serveur de journalisation, mais elle respecte les principes les plus importants que sont la collecte des journaux de l'ensemble des équipements, la centralisation et l'archivage hors ligne.

B.2 Architecture de journalisation étendue/multi-sites

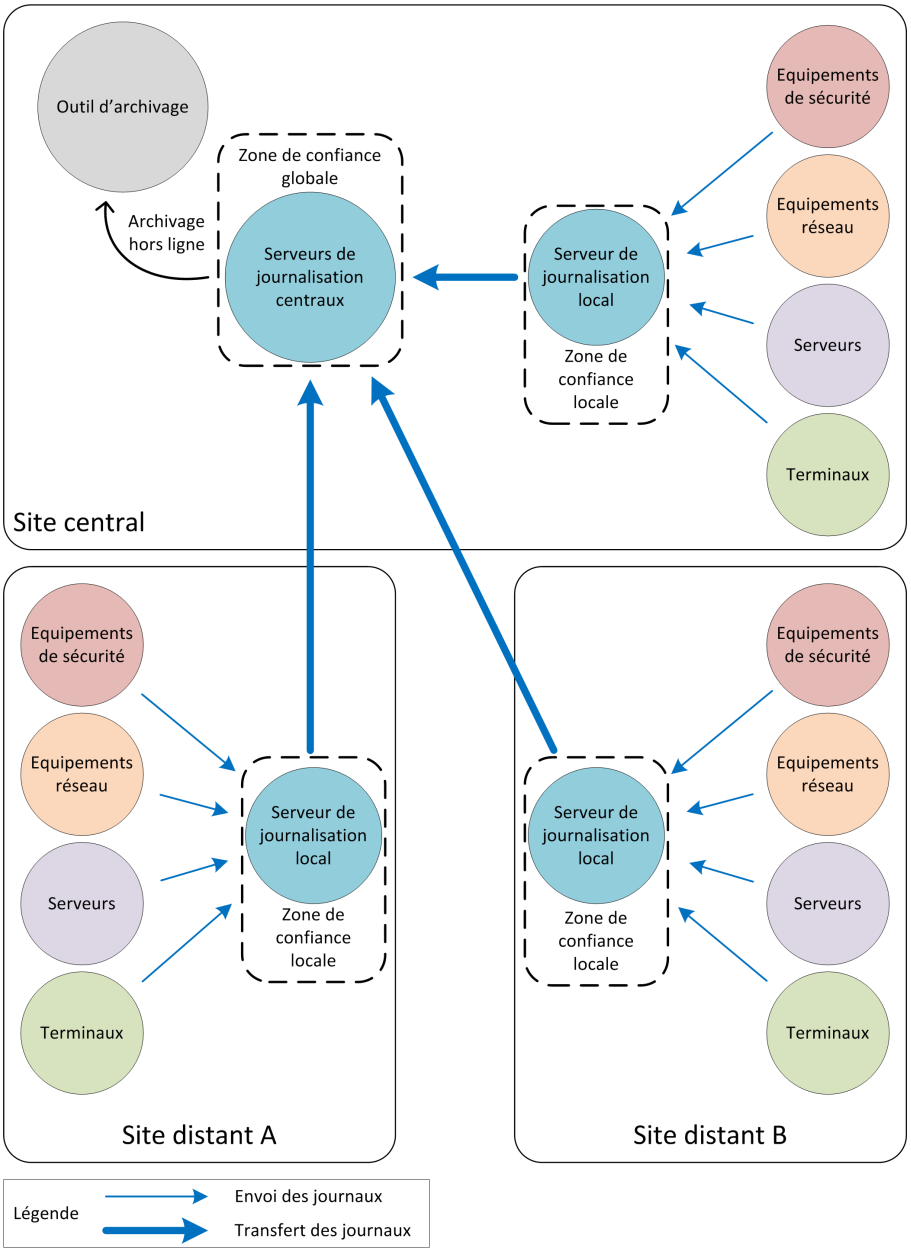

FIGURE 2 – Exemple d'architecture de journalisation multi-sites

Cette architecture plus complexe dispose de plusieurs serveurs centraux de journalisation, elle reprend les mêmes principes fondamentaux que l'architecture présentée précédemment. Elle montre aussi la nécessité d'étager les serveurs de journalisation lorsque les journaux de plusieurs sites ou de plusieurs entités sont collectés centralement. Ce type d'architecture permet de maîtriser les flux de communication entre les différents sites/entités. Il est à noter qu'il n'existe aucune interaction directe entre les équipements qui génèrent les journaux et les serveurs centraux, seuls des serveurs de journaux locaux peuvent communiquer avec les serveurs de journalisation centraux.

C Aspects juridiques et réglementaires

Les éléments juridiques et réglementaires sont structurants, ils doivent donc être pris en compte au plus tôt lors de la conception de l'architecture de journalisation. La réglementation pose un principe général d'effacement ou d'anonymisation des données de connexion. Elle édicte néanmoins plusieurs régimes juridiques distincts en fonction de la nature de celui qui opère la journalisation ou du cadre dans lequel les éléments de journalisation sont générés. Un tableau récapitulatif présent à la fin de cette annexe référence les textes législatifs et réglementaires principaux.

C.1 Valeur probatoire des éléments de journalisation

Un des objectifs des éléments de journalisation est de permettre la traçabilité de l'activité d'un réseau et d'apporter la preuve de cette activité (utilisation ou non-utilisation d'une application ou d'un service par un utilisateur, accès illégitime, etc.). Une partie non négligeable de leur intérêt réside dans leur capacité à identifier directement ou indirectement un individu ou un équipement ayant participé à cette activité. Afin d'être opposable en cas de contentieux, leur mise en œuvre doit respecter les règles relatives à l'administration de la preuve et les principes directeurs des procès civils et pénaux (loyauté, intégrité, licéité, etc.).

Signer et horodater les journaux dès leur création permet d'assurer leur intégrité et d'accroître leur valeur probatoire.

C.2 Régime général de protection des données à caractère personnel

Les éléments de journalisation peuvent contenir des données à caractère personnel, c'est-à-dire des données relatives à une personne identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification, ou à plusieurs éléments qui lui sont propres [6]. À la différence des données exclusivement techniques (numéro d'AS [7], nom de machine, etc.), une adresse de courriel, une URL ou une adresse IP sont régulièrement considérées par la CNIL [8] comme des données à caractère personnel.

Le traitement d'éléments de journalisation impose donc le plus souvent le respect des dispositions de la loi du 6 janvier 1978 et en particulier :

- la réalisation de formalités préalables auprès de la CNIL (déclaration, autorisation, etc.) ;
- la mise en œuvre d'un niveau de sécurité adapté aux données traitées et aux finalités ;
- la gestion du cycle de vie des éléments de journalisation (processus de création, de conservation, de destruction, etc.) ;
- et, le cas échéant, le respect des règles relatives aux flux de données transfrontaliers.

En outre, il est nécessaire de respecter les exigences relatives aux droits de la personne, qu'elles soient liées à la loi du 6 janvier 1978 (consentement préalable, droit d'accès, droit de rectification, etc.) ou à d'autres dispositions (protection de la vie privée, des correspondances privées, etc.).

La CNIL ainsi que la jurisprudence [9] ont posé plusieurs principes applicables à la gestion des éléments de journalisation par des personnes habilitées [10] (administrateurs, gestionnaires de compte,

6. Art. 2, loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
7. *Autonomous System* ou Système Autonome
8. Commission Nationale de l'Informatique et des Libertés
9. Voir notamment les deux jurisprudences : CA Paris, 11ème ch. 17 décembre 2001 et CA Paris, 14ème ch. 4 février 2005.
10. Le terme « habilité » est utilisé ici au sens juridique, c'est-à-dire « apte à accomplir un acte ».

etc.), par exemple :

- seules des personnes spécifiquement habilitées peuvent accéder aux éléments de journalisation ;
- l'accès doit être strictement limité à la finalité poursuivie, de la manière la moins intrusive possible pour les données à caractère personnel ;
- le personnel habilité est soumis à des obligations de confidentialité particulières et ne doit divulguer une quelconque donnée à caractère personnel que dans des cas limités liés au fonctionnement technique ou à la sécurité des systèmes ou aux intérêts de l'entreprise ;
- le personnel habilité ne doit subir aucune contrainte quant au dévoilement des informations, notamment par son employeur, sauf si la loi en dispose autrement (dans le cadre d'une procédure judiciaire).

Les éléments de journalisation ne peuvent être conservés que pour un temps limité.

Afin de satisfaire aux obligations relatives à la protection des données à caractère personnel, le gestionnaire des éléments de journalisation peut mettre en œuvre des mécanismes d'anonymisation. Afin de garder le caractère probatoire de l'élément de journalisation, l'anonymisation peut être réversible pour des finalités particulières.

Les activités liées à la gestion des éléments de journalisation doivent être strictement limitées au but poursuivi. Les procédures liées à la gestion des éléments de journalisation doivent être décrites dans des documents de référence, permettant ainsi de s'assurer que les données à caractère personnel ne sont pas conservées de manière illégitime.

C.3 Régimes particuliers relatifs à la conservation des éléments de journalisation

La réglementation encadre plusieurs hypothèses dans lesquelles certains opérateurs, en fonction de leur nature ou de leurs activités, sont astreints à une obligation de production et de conservation des éléments de journalisation. Le cas échéant, ces régimes sont cumulatifs.

C.3.1 Conservation des éléments de journalisation par les fournisseurs d'accès à Internet (FAI) [11] ou d'hébergement

Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication au public en ligne (c.-à-d. les FAI) ainsi que celles qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services (c.-à-d. les hébergeurs) détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Sont en particulier concernés les fournisseurs d'accès et hébergeurs professionnels, les entreprises et administrations qui donnent accès à Internet à leurs personnels dans le cadre de leur activité professionnelle, les entreprises et administrations offrant un service en ligne qui stocke des données fournies par leurs usagers, les fournisseurs de point d'accès au public (hôtels, restaurants, etc.), les cybercafés, les fournisseurs de services en ligne (blogs, réseaux sociaux, etc.).

Les fournisseurs d'accès à Internet et les hébergeurs doivent conserver leurs journaux au minimum durant un an.

11. Art. 6-II de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ; décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données.

La non-conservation de ces données par les fournisseurs d'accès à Internet et les hébergeurs est sanctionnée pénalement par une peine d'emprisonnement d'un an et de 75 000 euros d'amende [12].

C.3.2 Conservation des éléments de journalisation des opérateurs de communications électroniques [13]

Les opérateurs de télécommunications électroniques, c'est-à-dire 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, ont l'obligation de conserver certaines données de leurs abonnés. Ces opérateurs peuvent être similaires à ceux visés dans l'annexe C.3.1 (cybercafés, fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne Wi-Fi que ce soit à titre payant ou non) mais les éléments de journalisation faisant l'objet d'une conservation diffèrent.

Les trois catégories de données concernées sont les données utiles :
- dans le cadre de la facturation et du paiement des prestations de communications électroniques ;
- dans le cadre de la recherche ou de la poursuite d'une infraction ;
- dans le cadre de la protection des systèmes d'information de l'opérateur de communications électroniques.

Les types de données concernés par ces catégories sont précisés par la règlementation [14], mais ne sont pas exhaustifs :
- les informations permettant d'identifier l'utilisateur ;
- les données relatives aux équipements terminaux de communication utilisés ;
- les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- les données permettant d'identifier le ou les destinataires de la communication.

La durée minimale de conservation est d'un an pour les deux premières catégories de données et de trois mois pour les données conservées pour la sécurité des réseaux et des installations.

La non-conservation, le non-respect de la durée minimale de conservation et de l'anonymisation des données sont sanctionnés pénalement par une peine d'emprisonnement d'un an et de 75 000 euros d'amende [15].

C.3.3 Accès aux éléments de journalisation par les autorités judiciaires

Les autorités judiciaires peuvent demander que les opérateurs de communications électroniques, les fournisseurs d'accès à internet ainsi que les fournisseurs d'hébergement soient astreints à leur fournir les éléments de journalisation cités précédemment. Conformément au code de procédure pénale, ces informations ne peuvent être obtenues que par une réquisition écrite.

C.4 Surveillance des salariés

En fonction de leurs finalités, les éléments de journalisation peuvent être considérés comme un moyen de surveillance des salariés. Dans ce cas, ils doivent respecter les règles relatives au droit du

12. LCEN, art. 6 VI, al. 1).
13. Art. L 34-1 du code des postes et des communications électroniques.
14. Art. R. 10-12, R. 10-13 et suivants du code des postes et télécommunications électroniques.
15. Art. L 39-3 du code des postes et télécommunications électroniques.

travail [16]. Ainsi, leur mise en œuvre doit, en particulier, être proportionnée au but recherché et être préalablement portée à la connaissance des salariés et, le cas échéant, des instances représentatives du personnel.

Les personnels et leurs instances représentatives doivent être associés à la définition des processus de mise en œuvre des mécanismes de journalisation, en particulier s'ils sont utilisés à des fins disciplinaires.

C.5 Réglementations sectorielles

Les gestionnaires des éléments de journalisation peuvent également être assujettis à des exigences complémentaires liées à leur secteur d'activité, en particulier en matière de traçabilité et d'archivage ou lorsqu'ils exercent leur activité dans un secteur régulé :

- secteur bancaire : traçabilité des opérations bancaires et financières [17] ;
- secteur des jeux en ligne : traçabilité des données de jeux [18] ;
- secteur de la santé : traçabilité des accès aux données de santé [19] ;
- etc.

Il est recommandé d'effectuer un état des lieux de la réglementation sectorielle applicable.

16. Art. L 121-8, L 432-2, L 1121-1, L 1222-4, L 1321-4 al. 3 du code du travail
17. Réglementations Bâle 2, Sarbanes-Oxley, LSQ, etc.
18. Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, art. 31.
19. Articles R1111-1 à -15-1 du code de la santé publique créé par le décret n°2006-6 du 4 janvier 2006.

C.6 Récapitulatif

Régime juridique	Fondement	Public concerné	Type de données concernées (Durée de rétention)
Fournisseur d'accès Internet	Art. 6.II de la loi n°2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique ; du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne	Personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne	- Données de connexion permettant d'identifer les personnes à l'origine de la création de contenu (1 an)
Hébergeurs	Art. 6.II de la loi n°2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique ; du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne	Personnes assurant, même à titre gratuit, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services	- Données de connexion permettant d'identifer les personnes à l'origine de la création de contenu (1 an)

Régime juridique	Fondement	Public concerné	Type de données concernées (Durée de rétention)
Opérateur de communications électroniques	Art. 34-1 du code des postes et communications électroniques ; décret n°2006-358 du 24 mars relatif à la conservation des données des communications électroniques	Toute personne qui, au titre d'une activité professionnelle principale ou accessoire, offrant au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès à un réseau, y compris à titre gratuit	- Facturation et paiement des prestations de communications électroniques (1 an) - Recherche et poursuite d'une infraction (1 an) - Protection des SI de l'opération de communication électronique (3 mois)
Données à caractère personnel	Loi n°78 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Responsables de traitement de données à caractère personnel	- Données à caractère personnel (durée de conservation minimale)