La sécurité des données à caractère personnel

1 Généralités, définitions et concepts

1.1 La sécurité des systèmes d'information

De nos jours, tous les organismes, qu'ils soient gouvernementaux, privés ou autres, sont forcés de collecter, rassembler, et traiter de plus en plus d'informations pour parvenir à atteindre leurs objectifs respectifs.

L'ensemble de toutes les technologies, et ce, y compris les systèmes d'application et de soutien, utilisées par un organisme pour parvenir à élaborer, à traiter, à stocker, à acheminer, à présenter à qui de droit, au moment voulu et de la façon voulue, l'information nécessaire, et finalement aussi, à détruire cette information le moment opportun, constitue **le système d'information** de cette organisation.

L'information constitue un capital qui, comme tous les autres actifs importants, est nécessaire à tout organisme pour son activité et doit donc être protégée de manière appropriée.

Quelle que soit la forme prise par l'information, ou quels que soient les moyens par lesquels elle est transmise ou conservée, il faut qu'elle soit toujours protégée de manière suffisante.

Dans le contexte normatif, la sécurité de l'information recouvre par définition[1] **"tous les aspects concernés par la définition, l'obtention et la conservation de la confidentialité, de l'intégrité, de la disponibilité, de l'imputabilité, de l'authenticité, de la fiabilité et de la non répudiation de l'information et des équipements de traitement de l'information".**

Ces différents aspects, définis ci-après, sont souvent appelés attributs ou caractéristiques de sécurité. Ils désignent l'état de l'entité concernée, que ce soit des informations, des processus, des systèmes ou même des personnes. La sécurité représente donc l'état de protection qui résulte de l'ensemble des mesures prises et des moyens mis en œuvre pour préserver les caractéristiques de sécurité des entités face aux risques encourus.

Définie de cette façon, la sécurité de l'information devient un des aspects primordiaux de la qualité intrinsèque de cette information.

1.2 Les différents attributs intervenant dans la sécurité de l'information

La confidentialité est la propriété d'une information de ne pouvoir être accédée que par des personnes, entités ou processus autorisés et de ne pouvoir être divulguée qu'à des personnes, entités ou processus autorisés.

[1]Norme ISO/IEC 13335-1:2004 – Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for information and communications technology security management.

Cette possibilité d'accorder un accès sélectif aux informations doit être assurée tout au long de la vie de ces informations notamment au cours de leurs collectes, de leur conservation, de leurs traitements et de leurs communications.

En pratique, les seules personnes autorisées à accéder aux données à caractère personnel sont les personnes dont la fonction ou les activités professionnelles justifient cet accès.

Les degrés de confidentialité dépendent de la nature des informations.

L'intégrité couvre deux aspects différents : l'intégrité des informations et l'intégrité des systèmes et processus.

L'intégrité d'une information est la propriété de ne pas être altérée ou détruite de manière non autorisée, volontairement ou accidentellement.

L'intégrité d'un système ou d'un processus est la propriété de réaliser la fonction désirée de façon complète et selon les attentes, sans être altérée par une intervention non autorisée, volontaire ou accidentelle.

La disponibilité est la propriété des informations, systèmes et processus d'être accessibles et utilisables sur demande d'une entité autorisée.

L'imputabilité est la propriété qui garantit que les actions d'une entité sont tracées et attribuées à cette seule entité.

L'imputabilité assure de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité).

La non répudiation est la propriété d'une action ou d'un événement d'avoir bien eu lieu et de ne pouvoir être niée ou nié ultérieurement. Dans le domaine du courrier électronique, par exemple, la non répudiation est utilisée aussi bien pour garantir que le destinataire ne puisse nier avoir reçu l'information que pour garantir que l'expéditeur ne puisse nier avoir envoyé l'information.

L'authenticité est la propriété d'une entité d'être bien celle qu'elle prétend être.

L'authenticité s'applique tant aux personnes (utilisateurs) qu'à n'importe quelle autre entité (application, processus, système, etc.). Elle implique une identification, c'est-à-dire la reconnaissance d'une dénomination permettant de désigner l'entité sans équivoque.

La fiabilité est la propriété de se comporter et de fournir des résultats conformes aux attentes.

La fiabilité se définit aussi comme la propriété d'être digne de confiance. On parlera souvent de données fiables pour des données qui sont exactes, précises et reproductibles.

1.3 L'importance de la sécurité de l'information

Vu la dépendance croissante des organismes à leur système d'information, l'information a acquis une valeur prépondérante pour ceux-ci. Cette importance concerne non seulement toutes les informations traitées par l'organisme dans le cadre de ses activités, mais aussi toutes les autres informations nécessaires à celui-ci pour pouvoir poursuivre ses activités de manière appropriée en toute circonstance.

Jusqu'il y a peu, la sécurité des systèmes d'information ne concernait que des réseaux informatiques essentiellement fermés et construits autour de systèmes autonomes aux capacités souvent limitées. Elle pouvait dès lors se satisfaire de quelques règles relativement simples de sécurité informatique (physique et logique).

De nos jours, les profils des activités humaines se sont fortement modifiés notamment en raison de la prolifération des ordinateurs individuels, de l'ouverture d'Internet au grand public, de la diffusion rapide des nouvelles technologies de l'information et des communications. De plus, l'interconnexion de tous les réseaux, l'accessibilité de l'information et la complexité croissante des systèmes fragilisent cette information et les différents processus impliqués. Réaliser de manière adéquate des activités commerciales ou offrir valablement des services aux citoyens exige donc la mise en œuvre de mesures de sécurité adaptées à des dangers en perpétuelle mutation.

La sécurité des systèmes d'information ne peut donc plus aujourd'hui être uniquement assimilée à un ensemble de mesures palliatives face à des imperfections technologiques, mais doit bien devenir un mode de comportement à adopter par toutes les parties concernées en vue de répondre à des impératifs plus essentiels relevant de valeurs humaines et fondamentales.

1.4 La sécurité des données à caractère personnel

Le concept de protection des données à caractère personnel se distingue partiellement de la sécurité de l'information. En effet, les données à caractère personnel constituent non seulement des informations et peuvent donc être protégées en tant que telles mais, de par leur spécificité de données à caractère personnel, ces données ainsi que les traitements qui leur sont associés doivent de plus répondre à des caractéristiques définies dans la Loi vie privée.

Les données à caractère personnel doivent être :

- traitées loyalement et licitement ;
- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ;
- exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises

pour que les données inexactes ou incomplètes, soient effacées ou rectifiées ;

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.

Des mesures de gestion, techniques et opérationnelles, doivent être mises en œuvre par l'organisme afin de :

- déclarer préalablement à la Commission de la protection de la vie privée tous les traitements nécessitant une telle déclaration ;
- respecter les droits de la personne, notamment en matière de consentement, de vérification, de modification et de suppression ;
- tenir les données à jour, rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes ;
- s'assurer que tous les traitements effectués soient bien conformes aux finalités et conditions légales ;
- limiter l'accès aux données aux seules personnes qui en justifient le besoin par l'exercice de leurs fonctions ou du service ;
- • informer les personnes autorisées à accéder aux données de leurs devoirs en vertu de la loi et, le cas échéant, leur faire signer un engagement de confidentialité ;
- préserver dans le temps la protection requise pour les données à caractère personnel ;
- en cas de sous-traitance, répercuter toutes les obligations du responsable du traitement sur le sous-traitant à l'aide d'un contrat approprié.

De plus, ces mesures doivent assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

On peut donc dire que la protection des données à caractère personnel est un droit primordial dont l'exécution dépend de certaines mesures de sécurité, ou en d'autres mots, qu'une approche de la sécurité est nécessaire à la bonne protection des données à caractère personnel.

2 Comment élaborer un processus de sécurisation ?

2.1 Les processus généraux de sécurisation

Sécuriser avec efficacité, sans déployer des moyens disproportionnés nécessite une approche structurée et rigoureuse.

Différentes méthodes pour maîtriser la sécurité existent. Elles se composent généralement de trois grandes catégories de processus :

- une **gestion des risques** qui vise à identifier les principaux risques, à discerner ceux qui doivent être traités et ceux qui sont acceptables, à mettre en œuvre les moyens de sécurité traitant les risques encourus par les données à caractère personnel selon une échelle de priorité. Les processus de gestion des risques forment un cycle qui est à répéter selon les particularités des systèmes et des risques identifiés. La gestion des risques débouche sur des processus de définition ou de mise à jour de la politique de sécurité et, souvent, sur des adaptations de l'organisation et des procédures de manière à mieux prendre en compte les nouveaux risques et les mesures de sécurité mises en œuvre ;

- la **gestion quotidienne de la sécurité**, comprenant notamment des activités comme l'administration des dispositifs de sécurité, la gestion des autorisations, l'analyse des incidents détectés ;

- le **système de management visant à une amélioration continue de la sécurité**. Il existe plusieurs modèles de système de management de la sécurité de l'information (ISMS - Information Security Management System). Le plus connu est basé sur une structure PDCA (Plan – Do – Check - Act). Cette amélioration continue se justifie par la nécessité d'adaptation à de multiples facteurs d'évolution comme les modifications de l'organisme et des risques associés, les modifications dans les systèmes d'information, les nouveautés technologiques tant pour les systèmes opérationnels que pour les dispositifs de sécurité.

2.2 La chaîne du risque

Les différents éléments intervenant dans un processus de sécurisation sont :

Les biens de l'organisme

Les biens (le "patrimoine", les "actifs" ou les "avoirs") d'un organisme, c'est tout ce qui a une quelconque valeur pour lui ou, en d'autres mots, tout ce qui ajoute de la valeur à l'organisme, ou encore, tout ce dont la perte aurait pour conséquence de diminuer la valeur ou l'efficacité de l'organisme.

Dans le cadre de la sécurisation des données à caractère personnel, sont considérés comme biens les données à caractère personnel et toutes les ressources nécessaires à leur traitement correct comme :

- les biens matériels abritant les données (les bâtiments, les machines, le matériel informatique, etc.) ;
- les logiciels nécessaires au traitement des données (les applications et les programmes utilisés, les systèmes d'exploitation, etc.) ;
- les informations utilisées dans le cadre des traitements des données et pouvant être mémorisées sous différentes formes : dans des bases de données, sur des documents papier, etc.) ;
- l'infrastructure (les services de base nécessaires à l'organisme pour atteindre son but : énergie électrique, éclairage, communications, transports, ascenseurs, etc.) ;
- le personnel (les travailleurs de l'organisme, le personnel temporaire, etc.) ;
- les biens intangibles (la réputation, l'image de marque, les valeurs éthiques, etc.) ;
- les ressources financières nécessaires au bon fonctionnement de l'organisme.

Les menaces

Une menace, c'est tout événement inattendu ou inespéré susceptible de porter préjudice à un des biens de l'organisme et donc, de nuire à la protection des données à caractère personnel.

Les menaces peuvent être d'origine environnementale (incendie), technique (pannes de systèmes) ou humaine.

Les menaces d'origine humaine peuvent être accidentelles (erreurs, omissions, procédures inappropriées) ou délibérées (malveillance, intrusion, vol), d'origine interne (divulgation d'information) ou externe (espionnage industriel).

Les vulnérabilités

Une vulnérabilité est une faiblesse d'un bien ou d'un groupe de biens qui peut être exploitée par une ou plusieurs menaces (faute de conception, installation incorrecte). Dans beaucoup de cas, la vulnérabilité réside dans le défaut de protection du bien plutôt que dans le bien lui-même.

Une vulnérabilité en elle même ne cause aucun préjudice à l'organisation. C'est l'occurrence d'une menace, qui, profitant de la vulnérabilité et, le cas échéant, de circonstances particulières, occasionne un incident pouvant éventuellement engendrer des dommages.

Les incidents

L'incident est un événement imprévu ou non espéré qui peut entraîner des conséquences, éventuellement importantes.

L'incident de sécurité de l'information est tout événement inattendu ou non espéré, susceptible de

compromettre une activité ou la sécurité des informations de l'organisme (dysfonctionnement ou surcharge d'un système, erreur humaine, fonctionnement anormal ou inhabituel d'un logiciel ou d'un matériel). En soi, un incident n'est ni bon ni mauvais.

L'impact

L'impact est la conséquence d'un incident sur un ou plusieurs biens (des données à caractère personnel ne sont plus exactes, par exemple).

En sécurité de l'information, on fait souvent la différence entre la conséquence directe (dommage au système d'information, comme la modification d'un fichier, l'accessibilité à une donnée confidentielle ou l'arrêt intempestif d'un système) et l'impact indirect (préjudice subi par l'organisme ou par des tiers, comme l'utilisation malveillante d'une information confidentielle, décision erronée suite à une donnée inexacte).

Il n'existe pas toujours de relation directe entre les conséquences directes d'un incident et l'impact indirect sur l'organisme ou sur des tiers : la perte d'une donnée élémentaire peut avoir des conséquences majeures pour la personne concernée alors que l'effacement complet d'un système peut ne nécessiter que la restauration du système depuis une copie de sauvegarde convenablement exécutée.

Le risque

Le risque est la probabilité qu'une menace donnée exploite des vulnérabilités d'un bien ou d'un groupe de biens et donc occasionne un dommage à l'organisme (exemple : effacement d'un fichier par un virus). Il est mesuré en terme de combinaison de probabilité d'un événement et de ses conséquences.

Un risque est donc caractérisé par deux facteurs : la probabilité qu'un incident se produise et l'importance des conséquences directes et des impacts indirects potentiels.

Le risque peut aussi dépendre du facteur temps : après un incident, la situation peut se dégrader progressivement si l'on ne prend pas les mesures correctives suffisamment tôt (exemple : erreur de logiciel affectant une base de données, programme espion collectant des mots de passe, des clés cryptographiques ou des codes PIN). Un incident bénin au moment de sa survenue peut ainsi conduire à des situations catastrophiques.

Les mesures de sécurité

Les mesures de sécurité, appelées aussi "mesures de protection" ou "contrôles de sécurité" sont des procédés ou dispositifs susceptibles de réduire les risques. Les mesures de sécurité peuvent être efficaces de différentes manières : en diminuant les possibilités d'une menaces, en corrigeant les vulnérabilités ou encore en limitant les opportunités de conséquences directes ou d'impacts indirects. Il est aussi possible d'agir sur le facteur temps. En effet, en détectant mieux et plus tôt les incidents, il est possible d'agir avant une dégradation significative.

Le risque résiduel

Les risques résiduels sont les risques qui restent après le traitement du risque, c'est-à-dire après la mise en œuvre des mesures de protection.

2.3 Positionnement du problème

Utopie du risque nul

Comme on l'a vu précédemment, la sécurité est l'état d'un système pour lequel les sept caractéristiques de la sécurité, c'est-à-dire la confidentialité, l'intégrité, la disponibilité, l'imputabilité, l'authenticité, la fiabilité et la non répudiation sont préservées.

La sécurité est donc un état dans lequel les informations sont perpétuellement valides, où les infrastructures garantissent parfaitement l'intégrité des données et où il est toujours possible de détecter et de déjouer toutes les actions malveillantes se présentant.

Cet état de sécurité est évidemment un idéal impossible à atteindre. De nombreux facteurs rendent cet objectif irréaliste. Parmi ces facteurs, il faut citer notamment les inconnues et les incertitudes, l'erreur humaine, l'érosion progressive de certaines mesures de protection, les changements imprévisibles, la malveillance qui se présente souvent là où on l'attend le moins. Bien plus, une couverture idéale du risque exige des moyens financiers et humains, souvent hors de portée des capacités de l'organisme.

Gérer le risque

Il y aura donc toujours un risque avec lequel il faudra bien vivre et le seul paramètre sur lequel on puisse agir est le niveau résiduel de ce risque.

Dans ce contexte, la sécurité devient donc l'art de gérer le risque et, gérer la sécurité revient à gérer le risque et à déterminer où mettre le seuil au-delà duquel celui-ci est jugé inacceptable pour l'organisme et en dessous duquel, compte tenu des moyens disponibles, il va bien falloir l'accepter.

Chaque organisme étant unique, il va de soi que la définition du niveau de risque acceptable variera d'un organisme à l'autre et que ce niveau de risque acceptable sera la pierre d'angle de l'élaboration et de l'organisation du système de sécurisation adapté à chacun d'eux.

De ce fait, il n'existe pas de recette miracle définissant le minimum de mesures de sécurité standards pouvant être installées dans n'importe quelle organisme et lui garantissant le niveau de sécurité adéquat.

Les mesures de sécurité nécessaires devront donc être établies spécifiquement et individuellement par et pour chaque organisme, et ce, de façon à atteindre les objectifs de sécurité qui leur sont propres.

Pour gérer les risques de manière optimale, il faut donc que chaque organisme applique une méthode suffisamment rigoureuse et adaptée à son propre contexte.

Si la gestion des risques nécessite un cadre méthodique, elle exige aussi une réflexion relevant du bon sens et d'autres éléments doivent aussi être pris en compte.

La sécurité totale n'est jamais meilleure que celle du point le plus faible de l'organisation. La sécurité devra donc être considérée comme un problème global et être conçue de façon homogène sur l'ensemble du système d'information.

La sécurité ne consiste qu'en un ensemble de compromis. En effet, plus le niveau de sécurité désiré est élevé, plus les contrôles à mettre en place seront lourds et complexes, plus il faudra recourir à une administration compliquée, et moins les informations seront faciles à utiliser.

Ces compromis doivent aussi prendre en compte, non seulement les problèmes rencontrés, mais aussi l'importance financière des solutions proposées. Le coût de la mise en place des mesures de sécurité doit évidemment être évalué en comparaison de la valeur des biens à protéger et des conséquences que pourrait avoir un incident de sécurité dû à une absence de protection.

La démarche de gestion du risque sera donc celle du 'bon père de famille'.

Gérer le risque relatif aux données à caractère personnel

Lorsque des données à caractère personnel sont traitées, les exigences de la Loi vie privée doivent être traduites en termes d'exigences de sécurité de manière opérationnelle et concrète.

Pour cela, les données à caractère personnel devront être inventoriées et, pour chaque ensemble de données personnelles, des réponses devront être trouvées aux questions suivantes :

- confidentialité : quelles personnes, quels systèmes ou processus sont autorisés à accéder aux données ? Quand et à quelles conditions ?
- Intégrité et fiabilité : comment ces données sont-elles collectées ? Quelles personnes, quels systèmes ou processus sont autorisés à modifier ou à traiter ces données et à quelles conditions ?
- disponibilité : dans quel délai ou avec quelle échéance ces données doivent être accessibles aux personnes, systèmes ou processus autorisés ?
- éléments de preuve (authentification, imputabilité et non répudiation) : quels sont les éléments de preuve qui devront être produits, si nécessaire ?

2.4 La gestion du risque

Une bonne gestion du risque implique une succession de plusieurs activités.

Définir ses objectifs de sécurité

Il est essentiel qu'avant toute chose, l'organisme identifie et définisse clairement ses exigences de

sécurité ainsi que les priorités qu'il juge nécessaire d'appliquer à ces exigences et ce, en fonction de ses propres valeurs éthiques ou des priorités liées à sa mission.

Identifier, estimer et évaluer le risque

Identifier les risques consiste à définir des situations dangereuses qui, par défaut de sécurité, peuvent conduire à enfreindre les exigences de sécurité. Ce sont des situations qui, selon les événements, peuvent occasionner un dommage à l'organisme ou un préjudice à des tiers.

Estimer le risque revient essentiellement à déterminer la probabilité des conséquences d'un risque, compte tenu de circonstances propres à l'organisme comme les menaces à prendre en considération ou les vulnérabilités technologiques. L'estimation est une démarche systématique qui peut s'effectuer selon différentes approches. Certaines approches systématiques et rigoureuses reposent sur des méthodes formalisées qui peuvent parfois se révéler trop lourdes ou trop coûteuses compte tenu des circonstances. D'autres approches, plus simples, font appel à des niveaux de sécurité de référence. Il appartient à chaque organisme de faire le choix le plus approprié.

Évaluer le risque consiste à confronter le risque estimé aux critères propres à chaque organisme, comme ses priorités sociales, sa politique financière ou ses valeurs éthiques et aux différentes contraintes légales. Cette évaluation permet de déterminer les risques qui, dans l'absolu, doivent être traités en priorité.

Traiter le risque

Une fois tous les risques évalués, il faut décider comment les traiter ou au contraire les accepter.

Le traitement d'un risque consiste à choisir une ou plusieurs mesures de sécurité qui vont permettre de le réduire, d'en atténuer les conséquences ou de le supprimer complètement. C'est un examen des mesures de sécurité les plus appropriées, basé sur une analyse coûts/bénéfices qui permettra d'optimiser ce choix.

Certains risques peuvent être transférés, en les couvrant par une assurance, par exemple.

Les décisions de traiter les risques doivent s'établir selon une échelle de priorités. Les risques à traiter en priorité sont ceux dont le traitement nous est imposé par la loi ou toute autre contrainte (limiter l'accès aux données à caractère personnel est une exigence légale, par exemple). Viennent ensuite les risques qu'il est possible de réduire un maximum pour un coût moindre. Enfin, la basse priorité sera attribuée aux "petits" risques, n'ayant qu'une très faible probabilité de survenance ou des conséquences mineures.

Accepter certains risques

Certains risques connus ne peuvent être traités, parce que le traitement est techniquement impossible ou que le coût s'avère disproportionné, par exemple. Ces risques doivent faire l'objet d'une décision d'acceptation par la direction générale de l'organisme, justifiant le non traitement de ceux-ci.

Pour d'autres risques, il s'avère plus avantageux d'en gérer les conséquences uniquement lorsque le sinistre survient plutôt que de traiter le risque lui-même au préalable. A titre d'exemple, une grande base de données subissant peu de modifications pourra plus facilement être sauvegardée par une copie peu fréquente complétée par les informations des modifications successives plutôt que par une copie complète et fréquente de la totalité de celle-ci.

Gérer les risques résiduels

Les risques résiduels doivent faire l'objet d'un suivi. Une décision de les traiter peut être nécessaire si, suite aux circonstances, ils deviennent inacceptables ou si le coût de leur traitement devient envisageable ou justifié. Un risque non traité peut aussi devoir être traité suite à une nouvelle obligation légale.

Réaliser la communication relative au risque

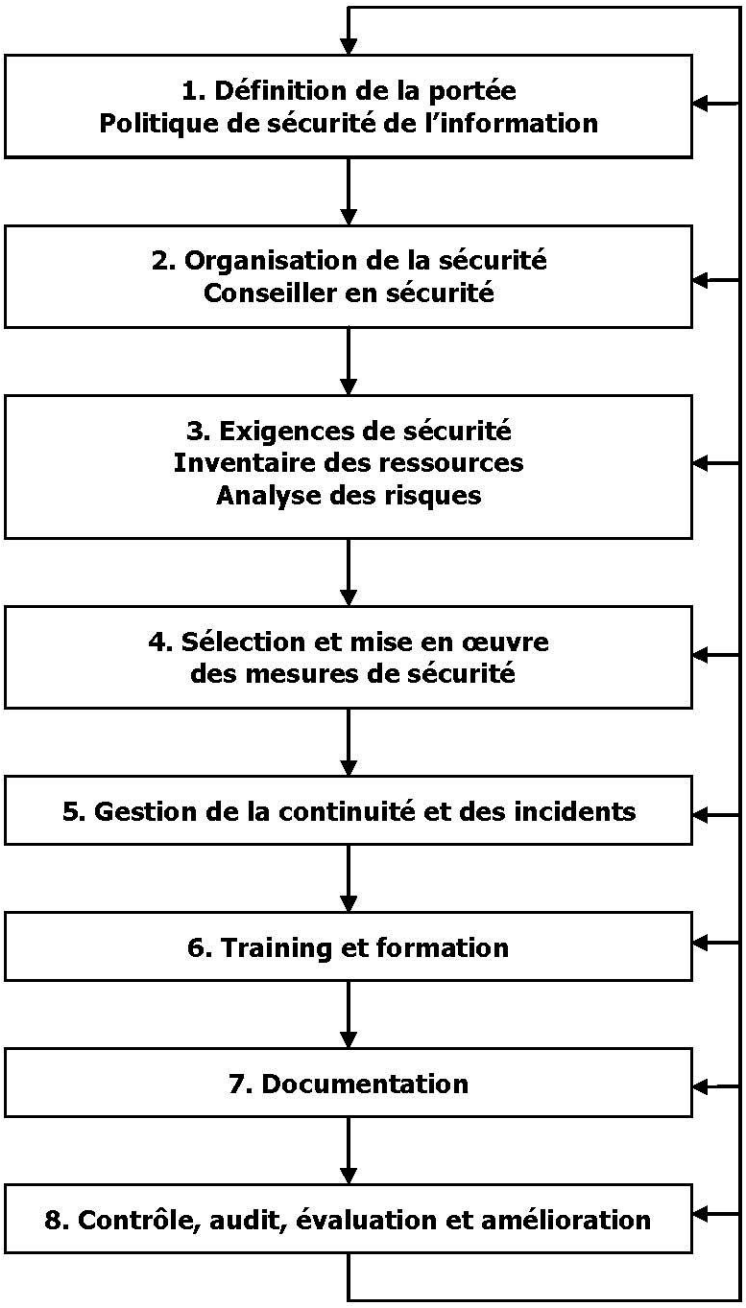
La communication relative au risque et à sa gestion doit être intégrée dès le départ au projet de sécurisation et accompagner celui-ci tout au long des différentes étapes de conception, d'élaboration, de mise en place et de maintenance de celui-ci. Dans tout organisme, chaque personne doit connaître les risques propres à ses activités, et plus particulièrement ceux relatifs aux données à caractère personnel. Chaque personne susceptible d'être confrontée à un risque de sécurité dans le cadre de ses activités doit être informée de ce risque, des mesures de sécurité en application et des règles à suivre pour préserver l'efficacité de ces mesures.

Effectuer le contrôle et le suivi

Tout au long des activités de l'organisme, les mesures de sécurité doivent faire l'objet d'un suivi et de contrôles. Il est en effet nécessaire de s'assurer que les mesures de protection des données conservent leur efficacité, que des nouvelles circonstances ne modifient pas l'un ou l'autre facteur intervenant dans l'appréciation des risques et que les incidents sont détectés au mieux. De plus, il faut vérifier que les toutes les décisions de correction ou d'amélioration ont bien été suivies des actions nécessaires, dans le délai attendu.

3 Approche générale de la sécurité de l'information

3.1 Approche générale



1. Revoir régulièrement la politique de sécurité de l'information et la diffuser dans l'organisme. La portée de la politique doit être définie en termes d'organisation, de localisation et de ressources.

2. Adapter l'organisation de la sécurité aux besoins en évolution avec une désignation claire des responsabilités, tâches et compétences.

3. Définir les exigences en matière de sécurité pour les ressources dans la portée de la politique de sécurité, réaliser un inventaire des ressources et une analyse des risques.

4. Sélectionner et mettre en œuvre les mesures de sécurité pour prévenir les risques.

5. Prévoir la poursuite des activités essentielles de l'organisme en cas de sinistre ainsi que la gestion des incidents de sécurité.

6. Prendre les mesures nécessaires afin que toute personne intervenant soit constamment suffisamment informée de ses devoirs et responsabilités et correctement formée à l'exercice de sa fonction et de ses responsabilités de sécurité.

7. Constituer toute la documentation nécessaire à la bonne gestion de la sécurité.

8. Prévoir la surveillance constante des mesures de sécurité mises en place afin de vérifier leur adéquation aux risques réellement encourus et organiser les éventuels correctifs nécessaires.

3.2 Rôles et responsabilités

Qui est responsable au sein de l'organisme de la sécurité de l'information ?

La sécurité informatique fut longtemps l'affaire des seuls départements technique et informatique qui n'avaient qu'à mettre en œuvre, chacun dans leur domaine, les moyens technologiques nécessaires à la protection des systèmes.

L'évolution de la sécurité et des différents moyens à mettre en œuvre implique aujourd'hui une approche beaucoup plus globale, notamment en ce qui concerne la protection des données à caractère personnel. L'efficacité des mesures de protection requises induit la responsabilité de toute personne susceptible d'influer sur la sécurité de chacun des éléments composant le système d'information soit en les concevant, soit en les développant, soit en les installant mais aussi et surtout, en les utilisant, c'est-à-dire, de nos jours, de quasi toutes les personnes composant l'organisme.

Un projet de sécurisation globale et cohérente d'un système d'information est donc une tâche permanente réclamant la participation de tous. C'est un travail sur mesure qui doit imprégner la culture d'entreprise et qui doit trouver le juste équilibre entre des intérêts souvent opposés de sécurité, d'impératifs opérationnels, de contraintes techniques, de convivialité pour les utilisateurs et de budgets pouvant y être affectés.

Un tel projet mobilisant toute l'organisation exige donc l'adhésion active et totale :

- de la direction générale de l'organisme pour définir la politique de sécurité et la mettre en application, pour organiser et distribuer les rôles individuels, affecter les moyens nécessaires, pour mettre en place les processus de gestion des risques, de décision de traitement des principaux risques et d'acceptation des risques jugés acceptables ; pour diffuser les règles et consignes de sécurité, pour les imposer au personnel de l'organisme et aux sous-traitants ; pour suivre les incidents et l'évolution du degré de sécurité afin de préserver le niveau de protection nécessaire, et enfin pour évaluer et sanctionner les éventuelles enfreintes de sécurité ;

- du personnel opérationnel de l'organisme (utilisateurs des systèmes) et des tiers concernés pour respecter les règles et consignes édictées et pour contribuer de manière active à la protection des données à caractère personnel ;

- des techniciens qui conçoivent le système d'information et les mesures de sécurité spécifiques, les développent, les installent et en assurent l'administration et la maintenance de façon à garantir que les données à caractère personnel bénéficient constamment du niveau de protection requis.

Dans cette organisation de la sécurité, certains rôles méritent d'être précisés :

Le responsable du traitement

C'est la personne juridiquement en charge du traitement des données, responsable de l'application de la Loi vie privée. Cette responsabilité relève de la direction générale de l'organisme, du conseil d'administration, ou du comité de direction selon les cas.

Le conseiller en sécurité du système d'information

Le conseiller en sécurité de l'information est le maître d'ouvrage de la sécurisation de l'organisme et le responsable de l'exécution de la politique de sécurité au sein de l'organisme.

Il doit définir les objectifs à atteindre, suivre et conseiller les différents intervenants à tous les niveaux de la mise en place du système de sécurisation et finalement vérifier les résultats.

Pour l'exécution de sa tâche de conseiller en sécurité de l'information, il rapporte directement à la direction générale de l'organisme et doit disposer des moyens suffisants (en temps, en ressources humaines et matérielles et en budget) et avoir accès, sans contraintes, aux informations nécessaires à sa fonction, pour autant qu'il reste dans le cadre de la politique de sécurité.

Il doit disposer des compétences et formations nécessaires et ne peut exercer de fonction(s) ou de responsabilité(s) incompatible(s) avec celles de conseiller en sécurité de l'information.

Il veille à ce que les différentes responsabilités en matière de sécurité (prévention, surveillance, détection et traitement) soient clairement identifiées et que les personnes en charge de la sécurité puissent agir en toute indépendance à l'abri des pressions d'intérêts particuliers et contradictoires.

Il devra, plus spécifiquement :

- être l'initiateur et le moteur de l'élaboration de la politique de sécurité de l'information et de sa traduction dans les diverses stratégies mises en place ainsi que son implication dans la définition des besoins en moyens (humains, financiers, matériels, etc.) ;

- être le principal animateur de la "culture de sécurité" ;

- être le principal conseiller en matière de sécurité de l'information à tous les niveaux (de la

direction générale aux utilisateurs) et pour toutes les différentes composantes concernées (sécurité physique des biens et des personnes, sécurité informatique, organisation interne, etc.) ;

- veiller à la transcription des contraintes légales et réglementaires en vigueur dans les solutions concrètes, tant sur le plan humain ou organisationnel que sur le plan technologique ;
- être le principal interlocuteur sécurité envers les tiers ;
- prendre les dispositions nécessaires pour la gestion des risques, valider les risques identifiés ainsi que l'évaluation des risques. Il secondera la direction dans les décisions relatives au niveau de risque
- acceptable, au traitement du risque (choix optimal des mesures de sécurité) et à l'acceptation de certains risques ;
- • traduire les exigences de sécurité de l'information en spécifications utilisables pour les développement, la mise en œuvre, l'utilisation, la maintenance, les changement et la suppression de tous les composants du système d'information (matériel, logiciel, ressources humaines, etc.) ;
- • valider les mesures de sécurité mises en place en place en s'assurant de leur efficacité ;
- • suivre les collectes de données et les traitements pour s'assurer du bon respect de la politique de sécurité, et cela dans les activités opérationnelles quotidiennes ;
- • détecter et analyser les incidents de sécurité de l'information, prendre les dispositions de corrections immédiates, de sanctions éventuelles et de corrections pour le long terme ;
- • faire effectuer les inspections et audits qui seraient nécessaires.

Le préposé à la protection des données

La Loi vie privée introduit la fonction de préposé à la protection des données et définit celui-ci comme étant chargé d'assurer d'une manière indépendante l'application de la loi et de ses mesures d'exécution[2].

Un futur arrêté royal doit détailler exactement les devoirs et responsabilités du préposé à la protection des données ainsi que son mode exact de fonctionnement.

[2] Loi vie privée, article 17bis.

3.3 La politique de sécurité

Objectifs

La politique de sécurité doit émaner de la direction générale et reprendre les lignes de conduite que l'organisme se propose de suivre en vue de maîtriser la sécurité de l'information et plus particulièrement la sécurité des données à caractère personnel.

La politique de sécurité doit être formulée par écrit de façon à pouvoir être communiquée de manière précise à chaque personne concernée aussi bien au sein de l'organisme qu'auprès des tiers concernés.

La politique décrit le niveau de sécurité à atteindre. Elle précise les droits et devoirs de l'ensemble des personnes concernées. Elle peut être complétée par des procédures décrivant le mode opératoire et des consignes à suivre dans des cas spécifiques.

Contenu

Une politique de sécurité doit comprendre au moins les éléments suivants :

- les fondements de la sécurité de l'information propres à l'organisme intégrant les obligations légale et les missions propres à l'organisme. La politique de sécurité précisera notamment les principes régissant la protection des données à caractère personnel ;
- les exigences de sécurité à respecter en termes de confidentialité, intégrité, disponibilité, imputabilité, authenticité, fiabilité et non répudiation des informations ;
- les différents éléments de sensibilisation aux arguments et au contenu même de cette politique définie par l'organisme ;
- la description des différents rôles, responsabilités et règles organisationnelles cadrant la mise en application de la politique de sécurité ;
- la démarche de gestion des risques adoptée par l'organisme afin de détecter les risques, de les apprécier selon des critères définis et de déterminer les modalités pour les traiter en les réduisant à un niveau acceptable ;
- la description du cadre organisationnel des processus de gestion des incidents de sécurité ;
- les modalités générales de gestion de la sécurité de l'information, notamment en matière de protection et de prévision ;
- les modalités retenues par l'organisme afin d'intégrer la politique de sécurité dans les processus de développement, de maintenance et de changement ;
- les dispositions de surveillance, d'évaluation et de mises à jour de la politique de sécurité et des différents composants de sécurité mis en place.

Souvent il est utile de préciser dans la politique les éléments suivants :

- les risques prioritaires qui nécessitent des mesures de sécurité ayant toute l'efficacité nécessaire ;
- les modalités de sensibilisation, d'information et de formation à la politique de sécurité, aux procédures et aux mesures de sécurité mises en œuvre ;
- les modalités de maintenance de la politique de sécurité de l'information, notamment pour les adaptations suggérées par des analyses d'incidents de sécurité ou pour la conformité à des lois plus récentes ;
- les modalités de contrôle des mesures de sécurité mises en place, notamment en matière d'inspection quotidienne ou d'audits périodiques ;
- certaines règles de bonnes pratiques susceptibles de construire la culture de sécurité qui doit se refléter dans les activités quotidiennes du personnel de l'organisme.

Cette politique devra être actualisée en permanence.

4 Les modèles de références

Élaborer un projet de sécurisation est un problème complexe qui ne peut être appréhendé sans une approche systémique. Plusieurs modèles de référence existent et peuvent être utiles afin de guider la réflexion lors de cette approche.

Les lignes directrices de l'OCDE[3]

Afin de promouvoir de meilleures réponses aux nouveaux enjeux et risques associés aux menaces pesant aujourd'hui sur les systèmes et réseaux d'information, le Conseil de l'OCDE[4] , a adopté le 25 juillet 2002 une Recommandation[5] aux États membres en vue de promouvoir une véritable culture de la sécurité basée sur neuf principes généraux auxquels devraient souscrire tous les processus de sécurité pour y parvenir.

Les neuf principes fondamentaux selon l'OCDE sont : la sensibilisation, la responsabilité, la réaction, l'éthique, la démocratie, l'évaluation des risques, la conception et la mise en œuvre de la sécurité, la gestion de la sécurité, la réévaluation.

---

[3] Disponibles à l'adresse suivante : http://www.oecd.org/dataoecd/16/22/15582260.pdf.

[4] L'OCDE, l'Organisation de Coopération et de Développement Économiques, est une organisation internationale regroupant 30 pays membres et ayant pour mission de renforcer l'économie de ses pays membres, d'en améliorer l'efficacité, de promouvoir l'économie de marché, de développer le libre-échange et de contribuer à la croissance des pays aussi bien industrialisés qu'en développement. La Commission des Communautés Européennes participe à ses travaux.

[5] Recommandation du Conseil de l'OCDE, 1037ième session du 25 juillet 2002 : 'Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information – Vers une culture de la sécurité'

La norme ISO/IEC 13335[6]

La norme ISO/IEC TR 13335 - Information Technology – Guidelines for the Management of IT Security (GMITS) se veut être un guide destiné au management destiné à assister celui-ci dans le choix des moyens de sécurité à envisager selon certaines caractéristiques de son système d'information.

La norme ISO/IEC 27002[7]

La norme ISO/IEC 27002 (remplace la norme ISO/CEI 17799 depuis le 1er juillet 2007) – 'Code of Practice for Security Management' nous fournit un exemple de catalogue de bonnes pratiques de sécurité qui peut être très utile comme référentiel de base lors de l'élaboration d'un processus de sécurisation.

Il va de soi, cependant, qu'un tel guide, élaboré au niveau général et international ne peut se permettre de détailler toutes les solutions pratiques et définitives à chacun des problèmes de sécurité possibles ni de tenir compte de la culture ou de la législation propre à chaque pays ou secteur d'activités.

Cependant, cette norme peut être considérée comme un bon guide, une bonne liste de contrôle énumérant, toute une série de bonnes pratiques courantes qui devront évidemment, chaque fois, être adaptées aux spécificités légales ou autres ainsi qu'aux besoins réels de l'organisation pour fournir une protection adéquate.

Les mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel'

Afin d'aider le responsable de traitement dans sa démarche de sécurisation des données à caractère personnel qu'il envisage de traiter ou qu'il traite, la Commission vie privée a publié les 'mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel', qui reprennent une liste de domaines d'actions liées à la sécurité de l'information pour lesquels tout responsable de traitement doit prendre des mesures qu'il doit évidemment adapter à son propre contexte et à ses propres spécificités.

---

[6] Peut être consultée gratuitement ou achetée à la bibliothèque du NBN (Bureau belge de normalisation : http://www.ibn.be) ou achetée sur le site de l'ISO : http://www.iso.org.

[7] Peut être consultée gratuitement ou achetée à la bibliothèque du NBN (Bureau belge de normalisation : http://www.ibn.be) ou achetée sur le site de l'ISO : http://www.iso.org.

5 Conclusion : les grands principes

Entamer un processus de sécurisation en suivant les grands principes :

- **La sécurité est une dimension essentielle de la qualité intrinsèque recherchée par l'organisation**

Sans la sécurité, il est impossible à toute organisation de fournir un produit ou un service de qualité suffisante. C'est, en quelque sorte, le niveau de la qualité recherché par l'organisation qui déterminera le niveau de sécurité nécessaire au sein de celle-ci.

- **La sécurité est une affaire de culture**

Elle exige un changement fondamental de la culture de l'organisation, et ce, notamment dans la manière dont cette organisation se comporte avec les informations qu'elle traite.

- **La sécurité demande une approche systémique**

La sécurité est un tout. Ce n'est pas une série d'incantations ou de recettes spécifiques qu'il suffit d'appliquer pour en être quitte. La sécurité des systèmes d'information dépasse largement le cadre de la simple mise en place de solutions techniques ou de l'achat de certains produits. C'est un problème qui doit être considéré dans son ensemble et toute solution de sécurité doit être élaborée globalement et avec cohérence.

- **La sécurité demande une approche 'consciente'**

Il est essentiel que toute solution de sécurité soit choisie en pleine connaissance de cause. Il est totalement improductif de choisir des solutions de sécurité toutes faites à l'aveuglette. Même dans le cas d'un transfert de risque chez des tiers, la sécurisation réalisée par ces tiers doit être pleinement comprise par l'organisation.

- **La sécurité doit poursuivre des objectifs**

On ne fait pas de la sécurité parce qu'il faut, ou pour sacrifier à une mode. On fait de la sécurité parce qu'on veut atteindre certains objectifs bien précis et ces objectifs doivent être clairement définis dans la politique de sécurité de l'organisation.

- **La sécurité est certainement d'abord une affaire de direction**

L'élaboration et la mise en place d'un processus de sécurisation efficace requiert la pleine conscience de la direction et des différents responsables, dont notamment le responsable de traitement, du rôle primordial que joue la sécurité au sein de l'entreprise ainsi que leur totale adhésion aux objectifs de sécurité recherchés et leur collaboration active.

- **La sécurité est ensuite l'affaire de tous**

Tous les membres de l'organisation, quels qu'ils soient, font tous partie, un moment ou l'autre, de la chaîne de sécurité et risquent, de ce fait, d'en être un jour le maillon faible. Chacun doit être conscientisé et responsabilisé de son propre rôle dans cette chaîne, et doit être préparé, éduqué et formé en conséquence.

- **La sécurité absolue est un mythe**

Il ne faut pas avoir la paranoïa de la sécurité à 100%. Elle n'existe pas. Il faut lui préférer un système de protection suffisamment dissuasif, à plusieurs niveaux de risque, chacun étant adapté aux différents niveaux de dangerosité des risques tels qu'ils sont perçus par l'organisation.

- **La sécurité est un processus permanent**

La sécurité n'est jamais un résultat acquis. Il faut sans cesse en assurer la maintenance, la remettre en cause et l'adapter aux modifications environnementales, à l'obsolescence, ainsi qu'à l'évolution des technologies.

Mais surtout avec beaucoup de bon sens :

- **Il faut sécuriser juste assez, mais pas plus**

Il faut sécuriser uniquement si le risque existe réellement pour l'organisation. Il ne faut pas sécuriser pour le plaisir de sécuriser. En sécurité, plus que partout ailleurs, le zèle doit être considéré comme suspect. Une mesure de sécurité inutile, puisque le risque n'existe pas, ou est insignifiant dans cet environnement, provoque des coûts et des lourdeurs inutiles pour cette organisation.

- **La sécurité doit être proportionnée**

Les moyens mis en place doivent être 'raisonnables' et proportionnés par rapport à ce qu'il faut protéger. Il doit nécessairement y avoir compromis entre la valeur du bien à protéger et le coût de la protection.

- **La sécurité, c'est 20% de technique et 80% de bon sens**

Bien avant la technique, la sécurité est avant tout une problématique d'organisation. Et sans les 80% de bon sens, les 20% de technique ne servent pas à grand chose. Il est donc peut-être plus sage de s'occuper d'abord des problèmes d'organisation, peu coûteux, avant d'aborder les problèmes techniques.

- **La loi de Pareto[8] se vérifie aussi en sécurité**

80% de la sécurité recherchée peut déjà être obtenue en mobilisant uniquement 20% de l'effort total nécessaire, alors qu'il faudra utiliser les 80% restants de cet effort total pour ajouter uniquement les 20% de sécurité supplémentaires.

[8] Vilfredo Pareto (1848-1923) Économiste italien.

- **Plusieurs mesures simples sont tout aussi efficaces qu'une mesure lourde et compliquée**

Comme le démontre le Théorème de Bayes[9]9, la combinaison de plusieurs mesures de protection simples, mais de ce fait peu performantes et bon marché, donne un tout aussi bon résultat qu'une seule mesure hyper performante mais alors vraisemblablement très coûteuse et difficile à mettre en œuvre (4 mesures efficaces à 70% combinées équivalent à une mesure efficace à 99%, par exemple).

- **Le danger vient de l'intérieur**

Comme le confirme toutes les études, 10% seulement des attaques proviennent de l'extérieur de l'organisation alors que 90% provient de l'organisation elle-même.

- **Le maillon le plus fragile des systèmes de sécurisation, c'est l'homme**

Les systèmes de sécurisation les plus complexes peuvent être mis en place, ils ne serviront à rien si le personnel n'en respecte pas les procédures ou le secret.

- **Avant tout, s'informer et se former**

La sécurité n'étant pas une donnée statique, elle nécessite un processus permanent d'information et de formation afin d'être constamment apte à en maîtriser les nouveaux défis.

Et en intégrant les principes nécessaires de protection des données :

- **La protection de la vie privée est un droit fondamental dont l'exécution dépend de la sécurité.**

Cette perception des choses doit constamment éclairer, diriger et imprégner toute démarche de sécurisation.

Pour cela, il faut avant tout que les objectifs de protection de la vie privée inhérents à l'organisation fassent, dès le début, partie intégrante de la politique de sécurité de cette organisation et obtiennent donc la même totale adhésion de tous, ainsi que la même diffusion, le même traitement et le même soutien que tous les autres objectifs de cette politique.

De plus, dans cette démarche de sécurisation, simultanément à tous les autres problèmes de sécurité traités, toutes les mesures seront prises afin d'assurer l'intégrité, la confidentialité et la sécurité des données à caractère personnel concernées.

[9] Thomas Bayes, (1702 – 1761), théologien et mathématicien anglais.