Chapitre 4
Sécuriser les traitements

1. Introduction

L'évolution des technologies de l'information (Cloud computing, Big Data, médias sociaux, etc.), la prolifération et la puissance des outils technologiques, le succès d'Internet et la multiplication des acteurs du secteur ont pour conséquence un foisonnement exponentiel des collectes et des traitements de données à caractère personnel. En parallèle, les menaces pesant sur les systèmes et réseaux d'Information sont de plus en plus nombreuses (fraude informatique, captation frauduleuse, perte de données, atteinte à la confidentialité, à la vie privée, etc.) et diverses (internes, externes). Le système d'information est dès lors utilisé comme vecteur de ces menaces qui consistent à viser le fonctionnement de ce dernier et/ou les données qu'il contient.

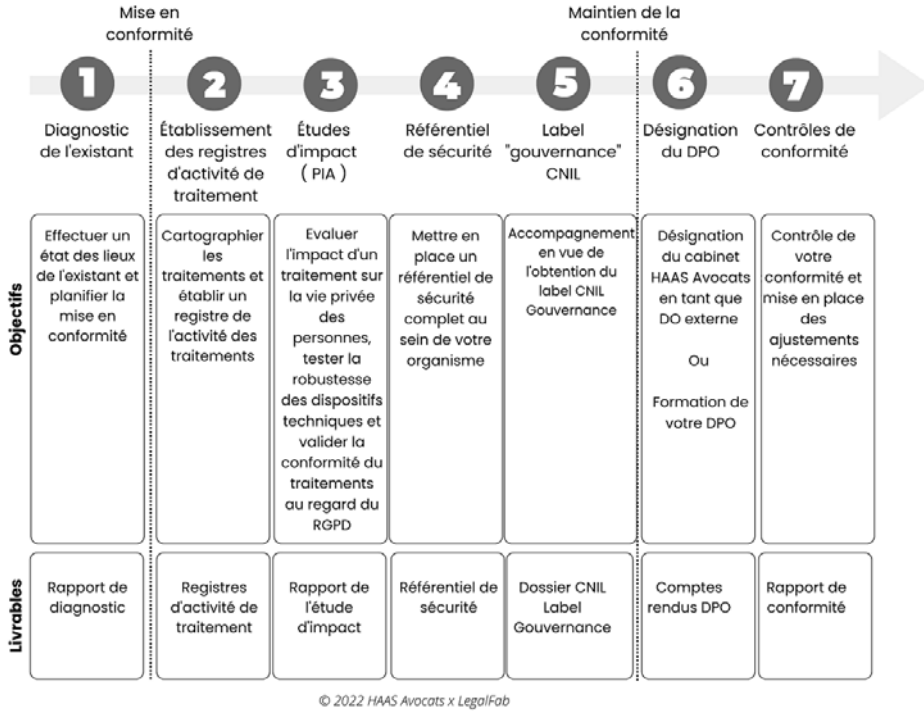
Soulignons qu'il n'existe pas de définition légale de la sécurité. Toutefois, l'agence nationale de la sécurité des systèmes d'information (ANSSI) définit la sécurité des systèmes d'information comme « *l'ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre et qui rend accessible* » (Défense et sécurité des systèmes d'information-Stratégie de la France, ANSSI 2011, p. 21 & 22).

La CNIL a d'ailleurs récemment rappelé que la cybersécurité du Web français était une thématique prioritaire (et a contrôlé en ce sens vingt-et-un organismes en 2021 pour, au final, en mettre quinze en demeure pour des défauts de chiffrement des données ou de gestion et de sécurisation de comptes d'utilisateurs (CNIL – Cybersécurité : 15 mises en demeure à l'encontre de sites web insuffisamment sécurisés – 08/07/22)).

En effet, la CNIL avait annoncé que l'un de ses objectifs était de contrôler le niveau de sécurité des « sites web français les plus utilisés dans différents secteurs ». Pour ce faire, la CNIL se concentrera sur :

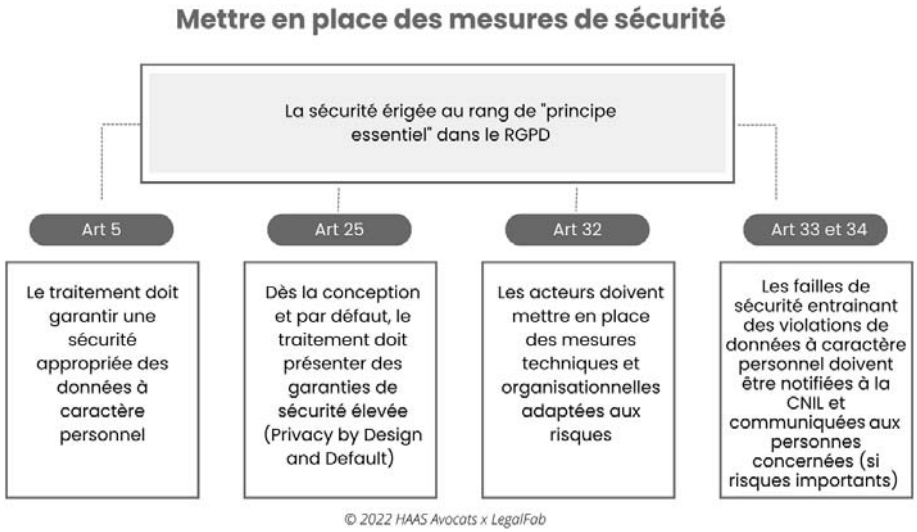
– les formulaires de recueils de données personnelles ;
– l'utilisation du protocole https ;
– la conformité des acteurs à la recommandation de la CNIL sur les mots de passe ;
– les stratégies mises en place pour se prémunir contre les rançongiciels.

(CNIL – Cybersécurité, données de santé, cookies : les thématiques prioritaires de contrôle en 2021 – 02/03/2021)



2. Qui est concerné par l'obligation de sécurité ?

Le RGPD, en introduisant une obligation générale de sécurité qui se traduit par la mise en œuvre des **mesures techniques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté au risque, érige la sécurité en pilier de la *Compliance*. L'objectif est ici de responsabiliser les différents acteurs des traitements de données en uniformisant les obligations pesant sur les entreprises (publiques ou privées). Ces nouvelles exigences sont valables pour les traitements futurs comme pour ceux déjà mis en place.



Tous les acteurs du traitement sont concernés par l'obligation générale de sécurité introduite par le RGPD, du responsable de traitement au sous-traitant qui doit désormais présenter « *des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* » (RGPD, art. 28).

Ces mesures visent à empêcher notamment toute diffusion ou accès non autorisé, la destruction accidentelle ou illicite, la perte accidentelle ou l'altération, ainsi que toute autre forme de traitement illicite.

Le devoir de sécurité comprend trois obligations distinctes : l'obligation de sécurisation, l'obligation de notification et l'obligation de communication, étant précisé que la deuxième et la troisième sont le prolongement de la première :

– L'obligation de sécurisation consiste à empêcher toute violation de données à caractère personnel, et d'une manière générale à limiter l'accessibilité aux données ;
– L'obligation de notification consiste à notifier à l'autorité de contrôle toute violation de données à caractère personnel ;

– L'obligation de communication consiste à communiquer toute violation de données à la personne concernée, si cela engendre un risque élevé pour les droits et libertés.

Le règlement indique différentes mesures techniques et organisationnelles à mettre en œuvre, selon les risques, en particulier la pseudonymisation et le chiffrement des données, la capacité d'assurer, de manière permanente, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services du traitement (RGPD, art. 32,33 et 34).

3. Pourquoi mettre en place des mesures de sécurité ?

Comme nous venons de le souligner, la sécurité constitue un élément de conformité incontournable et la plupart des acteurs du traitement devront accroître leur dispositif existant pour se mettre en conformité. Mais outre le volet légal, la sécurité doit aussi être abordée sous le volet économique, avec l'explosion du cyber-risque dont le montant du préjudice est de plus en plus élevé chaque jour. Nous vivons en effet dans une société du tout numérique, du tout connecté, du tout partagé. Mais derrière l'accroissement de la facilité d'accès aux données se cache l'accroissement des failles de sécurité possibles. Imaginez un voleur face à une première maison comprenant une porte d'entrée blindée, et une seule fenêtre protégée par des barreaux de fer, et une seconde maison avec trois portes d'entrée, deux baies vitrées, et une flopée de fenêtres ouvertes. À votre avis, où va-t-il aller ? Le problème est exactement le même en matière de sécurité informatique, et la recette du butin peut être très juteuse. D'après l'IBM Security Cost of a Data Breach Report 2021, les coûts des violations de données sont passés de 3,86 millions USD à 4,24 millions USD, soit le coût total moyen le plus élevé de l'histoire du rapport. Les coûts ont été :

– largement inférieurs pour plusieurs organismes ayant une stratégie de sécurité plus aboutie ;
– et plus élevés pour les organismes ayant pris du retard dans des domaines tels que la sécurité (IA), l'automatisation et la sécurité du cloud.

Il est intéressant de noter que le coût moyen des violations de données est supérieur de 1.07 million USD dans le cas où le télétravail était impliqué dans lesdites violations.

Ce même rapport estime que les données à caractère personnel des clients sont également les plus coûteuses, à 180 USD par fichier perdu ou volé. Le coût moyen global par donnée dans l'étude de 2021 était de 161 USD, une augmentation par rapport aux 146 USD par fichier perdu ou volé évoqué dans le rapport de 2020.

À l'échelon français, dans son « Panorama de la menace informatique » 2021, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) observe une amélioration constante des capacités des acteurs malveillants. Ainsi, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37 % entre 2020 et 2021 (786 en 2020 contre 1082 en 2021, soit désormais près de 3 intrusions avérées par jour).

La CNIL elle-même précise que 5037 notifications de violation de données ont été reçues en 2021 soit une augmentation de 79 % par rapport à 2020. Le fort impact des rançongiciels dans les crises de cybersécurité se confirment dans la mesure où 43 % de ces notifications concernent une attaque par rançongiciel (CNIL – Cybersécurité : 15 mises en demeure à l'encontre de sites web insuffisamment sécurisés – 08/07/22). Cette tendance ne semble pas près de stagner et des mesures de sécurité fortes doivent nécessairement être mises en place pour protéger le patrimoine informationnel de l'entreprise. De plus, les préjudices pour les entreprises sont multiples : atteinte à la réputation et à l'image, perte de confiance des utilisateurs, perte d'un savoir-faire, perte d'un avantage concurrentiel à la suite de diffusion de données stratégiques…

Il est dès lors primordial pour une entreprise de prévenir les risques qui pèsent sur ses systèmes d'information et de prendre des mesures correctives et préventives afin d'endiguer ces derniers. À ce titre, elle doit veiller à la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information et dans certains cas également de l'authenticité, de l'imputabilité, la non-répudiation et la fiabilité de cette dernière.

Un risque est caractérisé par trois composantes :

– la menace ;
– les vulnérabilités ;
– les impacts.

Atteintes aux données

La sécurité informatique ne se mesure que par sa résistance à une menace ou à une faille dans son système de traitement. L'attaquant (cracker ou hacker) cherchant avant tout à porter atteinte à l'état du système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

L'**atteinte à la disponibilité** réside dans le fait que les données (annuaire des fournisseurs, dossier patient, inventaire de pharmacie…) ou les traitements (application, web service, composant logiciel…) soient inaccessibles au moment prévu pour leurs usages autorisés.

L'**atteinte à la confidentialité** se caractérise par la mise à disposition non-autorisée de données qui deviennent accessibles à des utilisateurs non-habilités à les consulter.

Chapitre 3
Un système de management

1. Introduction

Ce chapitre décrit un système opérationnel de management des données à caractère personnel dont le but est de permettre à toute entreprise, quels que soient sa taille, son secteur, de respecter dans le temps les exigences du RGPD et de pouvoir le démontrer.

Au préalable, il nous semble utile de définir les termes suivants :

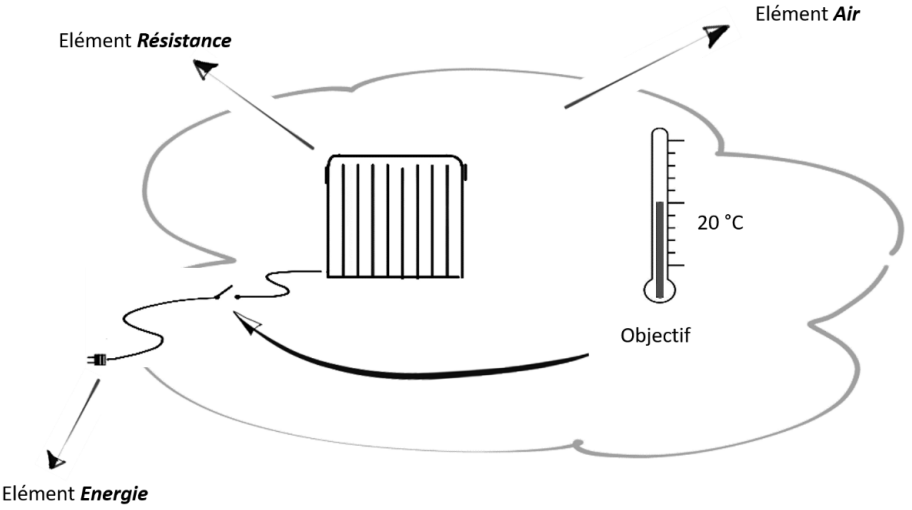
– Mesurer, c'est obtenir expérimentalement une ou plusieurs valeurs que l'on peut raisonnablement attribuer à une grandeur de même nature.
– Évaluer, c'est porter un jugement sur les valeurs mesurées.
– Contrôler, c'est vérifier le respect des procédures pour rechercher la conformité ou la régularité de celles-ci. Lorsqu'un écart est constaté, des actions correctives sont à mener.
– Piloter, c'est conduire vers un objectif.

2. Le système de management

2.1 Qu'est-ce qu'un système ?

Un système est un ensemble d'éléments interagissant entre eux de manière dynamique et en fonction d'un objectif. Pour assurer sa régulation, il dispose d'une boucle de rétroaction, appelée aussi feedback, qui permet de mesurer l'atteinte de l'objectif et d'agir en retour.

Exemple : votre système de chauffage comprend plusieurs éléments, à savoir l'énergie électrique, la résistance électrique du radiateur et l'air, qui interagissent. Dans ce système, si l'objectif est de maintenir une température ambiante de 20°, la fonction feedback est assurée par un thermostat d'ambiance qui actionne un interrupteur pour laisser passer le courant dans la résistance lorsque la température mesurée est au-dessous des 20° ou bien pour le couper lorsque celle-ci est au-dessus.



Système de chauffage

2.2 Qu'est-ce qu'un système de management ?

Les modalités de gestion d'une entreprise par sa direction constituent « l'art de manager ». Ces modalités font souvent partie de la culture et de la tradition orale de l'entreprise. Cela est particulièrement vrai pour les petites et moyennes entreprises, dans lesquelles les employés savent tous comment faire leur travail bien que peu de choses soient documentées. Disposer de politiques et procédures correctement documentées permet de s'assurer que chacun a bien connaissance des opérations qu'il doit réaliser pour contribuer à l'atteinte des objectifs de l'entreprise. Cette approche qui vise à objectiver, à structurer, à documenter et à communiquer les modalités de gestion d'une activité ou de plusieurs activités constitue un système de management.

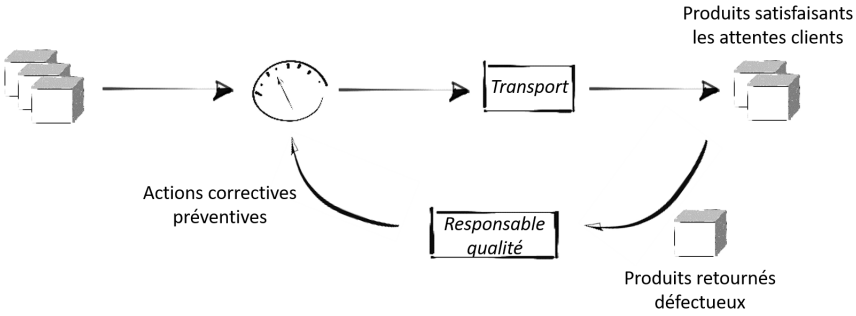
Selon l'ISO (Organisation internationale de normalisation), les systèmes de management permettent aux organismes de mettre en œuvre une démarche structurée dans leurs activités afin d'atteindre leurs objectifs.

Voici quelques exemples de systèmes de management :

Norme	Domaine	But
ISO 50001	Énergie	Pour faire un meilleur usage de l'énergie.
ISO 9001	Qualité	Pour que les produits et services soient constamment en phase avec les attentes des clients.
ISO 14000	Environnement	Pour maîtriser la responsabilité environnementale de l'entreprise.
ISO 27001	Sécurité de l'information	Pour assurer la sécurité des informations de l'entreprise.
ISO 27701	Protection de la vie privée	Extension d'ISO 27001 au management de la protection de la vie privée.

Il est probable que vous ayez déjà été concerné par un système de management de la qualité. C'est sans doute le système de management le plus répandu au monde. À partir d'objectifs de qualité ou de satisfaction client, il permet à l'entreprise de s'organiser pour que le niveau de qualité d'un produit ou d'un service soit conforme aux attentes des clients.

Exemple : une entreprise définit son taux de retour de produits défectueux. Celui-ci ne doit pas excéder 5 % du volume des ventes. Pour piloter cet objectif, l'entreprise effectue régulièrement des mesures. Au-dessous de 5 %, il n'y a pas d'actions spécifiques à mener. Au-dessus de 5 %, un contrôle est effectué pour identifier les causes de dépassement et des actions correctives et préventives sont à mener.



Contrôle qualité sur la chaîne logistique

2.3 Caractéristiques d'un système de management

Pour mieux comprendre ce qu'est un système de management, il nous paraît utile d'en donner ses caractéristiques. C'est à partir de ces caractéristiques que nous allons concevoir le système de management des données à caractère personnel (SMDCP).

Un système de management se caractérise principalement par :

– sa finalité
– son interaction avec l'environnement
– les objectifs pour arriver à la finalité

– les éléments qui le composent
– la fonction de contrôle ou de feedback
– sa politique
– le référentiel auquel il appartient
– ses propriétés, c'est-à-dire les qualités qui lui sont propres

3. Conception du SMDCP

Pour concevoir le SMDCP, nous avons considéré chacune des caractéristiques énoncées précédemment et nous les avons déclinées sur le domaine concerné.

3.1 Finalité du système

Il s'agit d'exprimer son but : pour quoi le système de management est conçu.

Dans notre cas, le système est conçu pour : permettre à l'entreprise de respecter dans le temps les exigences du RGPD et de pouvoir le démontrer.

3.2 Interaction du système avec son environnement

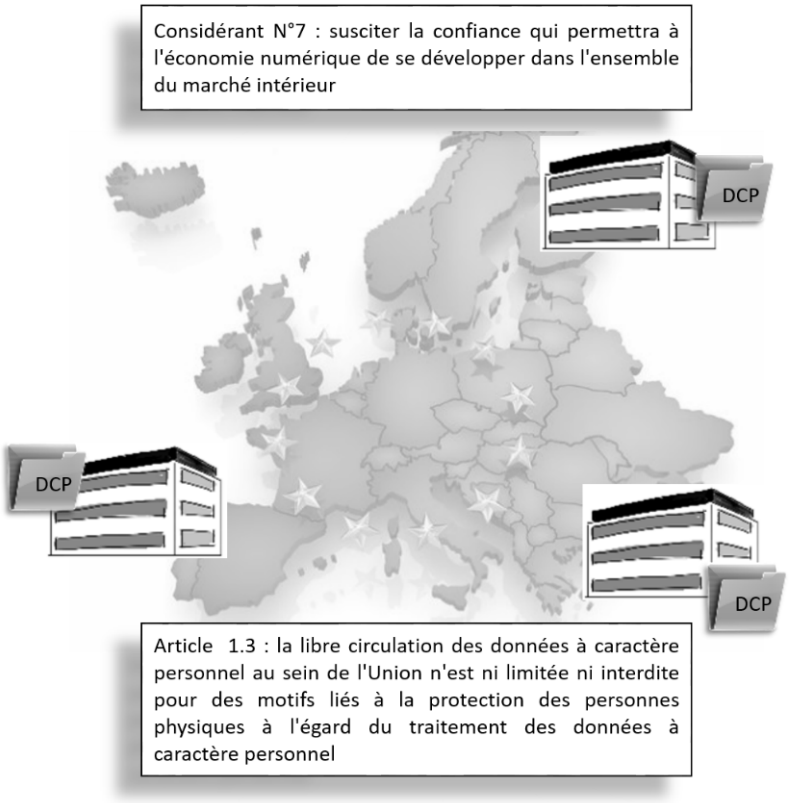
L'environnement considéré est celui du marché intérieur de l'Europe dans un contexte d'économie mondiale qui trouve principalement sa croissance dans le numérique. La libre circulation des données à caractère personnel est un des fondamentaux de cette nouvelle économie.

Cet environnement est pour partie résumé dans les considérants 6 et 7 ainsi que dans l'article 1.3 :

– L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. Ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur.

– La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Ce système doit accompagner la transformation numérique de l'entreprise pour lui permettre d'opérer légalement dans cette nouvelle économie.



Environnement

3.3 Objectifs du système

Une finalité du SMDCP qui se décline en objectifs.

Respecter dans le temps les exigences du RGPD et pouvoir le démontrer oblige l'entreprise à définir, à formuler et à combiner de multiples objectifs.

Pour définir et formuler les objectifs du SMDCP, nous avons analysé le contenu des exigences réglementaires. Nous en avons fait ressortir une trentaine. Nous les détaillerons un peu plus loin, mais à titre d'exemple en voici trois :

– Garantir que la gestion des droits de la personne concernée et les obligations réglementaires sont prises en compte dès la phase de conception d'un projet et durant son cycle de vie.
– S'assurer que tout le personnel traitant des données à caractère personnel a conscience de la pertinence et de l'importance de ses activités de traitement.
– Être organisé pour réagir en cas de violation de données.

Remarque

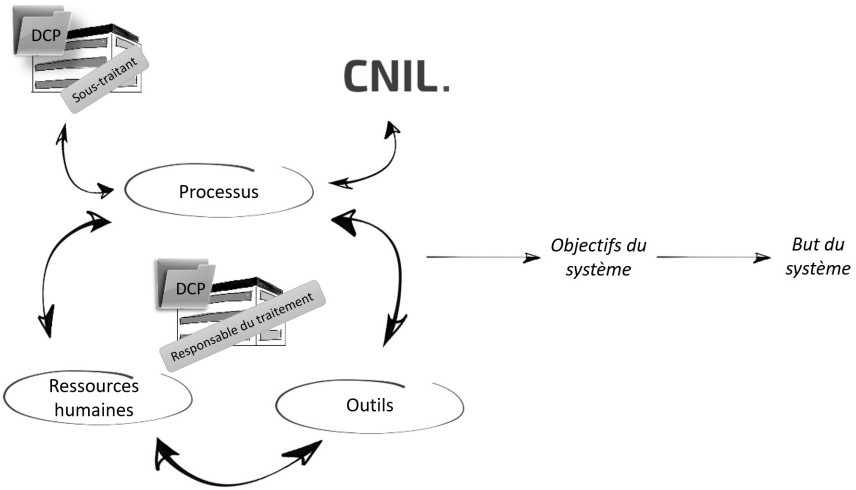
Le nombre et la formulation des objectifs sont à la libre appréciation du responsable du traitement.

3.4 Éléments qui le composent

Une fois les objectifs définis, nous pouvons déterminer les éléments qui composent le système, sa fonction de régulation, ses propriétés et ses règles de fonctionnement. Si les objectifs sont mal définis, le système sera mal conçu et il ne pourra atteindre son but.

Nos différentes expériences en matière de système de management organisationnel mettent en évidence trois types d'éléments qui interagissent entre eux :

– Des processus
– Des outils matériels ou immatériels
– Des ressources humaines



Trois éléments qui permettent de contribuer à l'atteinte des objectifs

3.5 Autres caractéristiques

Nous reviendrons plus loin sur les autres caractéristiques énoncées, car il nous semble important d'aborder dès à présent les éléments du système.

4. Processus du SMDCP

4.1 Définition

Un processus est un ensemble ou une succession d'activités réalisées à l'aide de moyens (personnel, informations, outils) pour atteindre un objectif.

Un processus peut se décomposer en plusieurs activités, qui elles-mêmes se décomposent en tâches.

La procédure est, quant à elle, une manière spécifiée d'effectuer les tâches d'un processus.