Fondements de dématérialisation et traitement des données sensibles: cadre d'étude sur l'impression bancaire.

Carole Henry, Sahbi Sidhom, Imad Saleh

Fondements de dématérialisation et traitement des données sensibles: cadre d'étude sur l'impression bancaire.

Carole HENRY [1], Sahbi SIDHOM [2] et Imad SALEH [3]
[1] : Université Paris 8, laboratoire Paragraphe, chenry05@etud.univ-paris8.fr.
[2] : Université de Lorraine, laboratoire Loria, sahbi.sidhom@loria.fr.
[3] : Université Paris 8, laboratoire Paragraphe, imad.saleh@univ-paris8.fr.

Résumé : L'externalisation du traitement des données sensibles est problématique et engendre la mise en place de procédures et d'habilitations particulières. Nous allons ici étudier la mise en œuvre de cette décentralisation des données dans le cas de l'impression des données bancaires et examiner les garanties proposées pour en assurer la disponibilité, l'intégrité et la confidentialité.

***Mots-clefs* — Certification, données bancaires, données sensibles, gestion des risques, normes, système d'information**.

I. INTRODUCTION

L'information sensible est décrite comme étant une information ou une connaissance qui par sa diffusion au public pourrait nuire aux entités auxquelles elle fait mention ou qui seraient concernées par son contenu. Cela peut concerner des aspects très variés comme la vie privée d'un individu, un échange commercial, la sécurité d'un état. La conséquence de cette diffusion est liée à la sensibilité et à la nature des éléments concernés. Nous reviendrons dans notre étude sur la présentation de ces différents concepts fondamentaux. Notre étude porte sur les difficultés de traitement des données sensibles pour préserver leur intégrité (cohérence, fiabilité et pertinence) et l'interopérabilité nécessaire entre les acteurs concernés. Nous étudierons le cas de l'impression externalisée des données sensibles bancaires au Luxembourg et la méthodologie déployée : la certification P.S.F (Professionnel du Secteur Financier).

Le problème posé par cette étude est la méthode de traitement des données sensibles dans le respect des principes de confidentialité que cela concerne l'émetteur, le contenu et le récepteur jusqu'à leur impression. Cette étude repose sur trois hypothèses de travail qui guideront cette analyse qui sont :

Comment traiter les données sensibles dans les contextes de systèmes d'information et des organisations ? Comment préserver la confidentialité des données sensibles jusqu'à leur impression ? Et enfin, quels sont les principes de dématérialisation pour la diffusion des données sensibles et comment le processus d'impression peut-il être optimisé ?

Nous évaluerons et analyserons les moyens mis en place et leur pertinence face aux enjeux majeures de leur traitement.

Nous étudierons dans un premier temps les concepts fondamentaux qui sont cristallisés autour de cette problématique, puis nous analyserons les usages des données sensibles au travers du rôle de la CNIL en France. Nous apporterons ensuite des informations sur le traitement et sur la gestion des risques informatiques. Le cas pratique de cette étude portera sur l'externalisation des données dans le domaine bancaire au Luxembourg avec la mise en place des certifications P.S.F.

II. CONCEPTS FONDAMENTAUX AUTOUR DU TERME « DONNEES SENSIBLES »

De nombreuses définitions du terme « données sensibles » confondent cette dernière avec la notion de données à caractère personnel. La « donnée à caractère personnel » est en fait un type de donnée sensible mais cette dernière ne résume pas le tout. Cette confusion provient du fait que l'on aborde ce sujet uniquement sous l'angle juridique. Il existe deux grands types de données sensibles : (i) les données sensibles non classées définies par la disposition interministérielle 901 [1] et (ii) les données sensibles classées « secret défense » (disposition interministérielle 1 300 [2]).

L'usage des termes « données sensibles » et « données à caractère personnel » n'a pas été transcrit de la sorte dans les usages. Nous avons constaté un amalgame fréquent dans le domaine opérationnel qui est celui de la confusion entre donnée et information. De cette manière, la classification proposée ci-dessous prend en compte le terme d'information classifiée et ne distingue pas ce qui est donnée de ce qui est information dans le modèle soumis.

Une « information classifiée » est une information sensible pour laquelle il est nécessaire d'obtenir une habilitation préalable pour y avoir accès. Ce type d'information est protégé et l'accès est restreint par la loi ou par le règlement à un groupe précis de personnes. Il s'organise selon un système hiérarchique du secret à plusieurs niveaux de sensibilité en fonction de l'importance des informations. Généralement tous les gouvernements utilisent ce type de classification. De manière globale « l'information sensible » est classée comme suit : l'information sensible, l'information classifiée qui comprend la notion de document, le secret industriel, le secret

professionnel, le secret bancaire, le secret médical en France, la raison d'État, le secret d'État.

Voici le classement qui a été réalisé et employé généralement pour ce type de données/informations dans les différents états. Il peut y avoir toutefois quelques nuances mais voici le modèle qui est généralement admis [14] [15] :

Appellation du niveau de classification	Traduction anglaise	Indications
Très secret	Top Secret	Il s'agit du plus haut niveau de sécurisation. Sa divulgation peut entraîner des conséquences exceptionnellement graves pour la sécurité nationale.
Secret	Secret	Sa divulgation peut entraîner des conséquences graves pour la sécurité nationale.
Confidentiel	Confidential	Sa divulgation pourrait nuire ou causer des effets préjudiciables pour la sécurité nationale.
Restreint	Restricted	Sa divulgation peut entraîner des effets indésirables pour la sécurité nationale. Il est à noter que tous les pays n'utilisent pas cette catégorie.
Non classifié	Unclassified	Utilisé pour les documents gouvernementaux qui ne nécessitent pas à une des classification présentées dans ce tableau. Ils sont accessibles sans habilitation particulière.

Tableau n° 1 : Modèle de classement des données dans les états

À cette recommandation s'ajoute le fait que certaines données non classées telles que les données et informations relatives à des domaines particuliers (médical, industrie, judiciaire, police, nucléaire, …) peuvent faire l'objet de mesures similaires. Ces cas plus spécifiques peuvent être traités dans le cadre des politiques de sécurité des ministères concernés. Du point de vue juridique et selon les principes érigés par la loi informatique et liberté de 1978 [3], les données sensibles font apparaître directement ou indirectement des informations concernant les origines raciales ou ethniques d'un individu, ses opinions ou appartenance politique ou syndicale ou religieuse, et tous les éléments sur sa santé ou son orientation sexuelle. Par principe la collecte ou l'usage de ce type de données sont très règlementés et ils doivent faire l'objet d'une demande auprès de la CNIL (Commission Nationale Informatique et Liberté) en France. La jurisprudence a étendue le champ de l'interprétation du terme « données sensibles ». « L'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, § 1, de la directive 95/46 » (CJCE, 6 nov. 2003). Tous les niveaux d'administration de gestion de données peuvent être concernés : un magasin qui collecte des informations sur ses clients pour réaliser des cartes de fidélité ou de démarchage commercial ; l'entreprise qui rédige un contrat de travail et qui tient un fichier de données à jour de ses employés sur son propre système informatique ou à défaut sur son ordinateur ; les données constituant les fiches de paie des salariés, une association ou un syndicat qui tient à jour une liste de ses membres… Il est toutefois à noter que pour les entreprises et pour les responsables de traitement, il existe parfois une confusion entre les informations dites stratégiques pour l'entreprise (données financières par exemple) et les données relevant du régime juridique des données sensibles telle que définit par la loi. [9] Par principe, la collecte et/ou l'usage de ce type de données sont très règlementés et doivent faire l'objet d'une demande auprès de la CNIL en France.

A. Usage des données sensibles : le rôle de la CNIL

Elle a en charge de veiller à ce que l'usage des données des individus ne porte atteinte « ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. » Elle a été mise en place dans le cadre de la loi Informatique et liberté et s'est vue octroyer de plus en plus de missions. Elle a le statut d'administration indépendante. La CNIL peut émettre des avis mais aussi des sanctions. Ces dernières peuvent faire l'objet de recours devant les juridictions administratives. La commission se réunit une fois par semaine et analyse principalement les décrets et textes de lois pour lesquels le gouvernement peut la solliciter pour émission d'un avis. Avec un effectif grandissant de 174 agents en juillet 2013, le Président de la CNIL a toute liberté pour les recruter. Chaque citoyen peut la saisir. Ainsi, la CNIL revendique 88 990 traitements déclarés, 6 017 plaintes, 3 682 demandes d'accès indirect aux fichiers de police et de renseignement, 458 contrôles, 43 mises en demeure, 9 avertissements et 4 sanctions financières pour un budget de 16 millions d'euros.

Dans ce cadre, elle détermine ses missions autour de cet axe « protéger la vie privée et les libertés dans le monde du numérique » autours de 6 objectifs :

- Informer les personnes sur leurs droits et leurs obligations ;
- Protéger les citoyens dans l'exercice de leurs droits ;
- Réguler et autoriser dans certains cas le traitement des informations sensibles ;
- Contrôler et vérifier si les traitements sont effectués dans le respect de la loi ;
- Sanctionner financièrement dans le cas du non respect de la loi par le responsable du traitement ;
- Anticiper et comprendre les évolutions techniques et technologiques.

Nous observons que la CNIL a un rôle déterminant permettant de contrôler et de sanctionner, si cela est nécessaire, en cas de manquements qui pourraient mettre en péril les données sensibles. La notion de risque est aussi présente dans la phase de traitement.

Le traitement des données sensibles impose un traitement particulier et des précautions particulières. Comment traiter les données sensibles dans le contexte de systèmes d'information et d'organisation ?

B. Traitement des données sensibles : gestion des risques informatiques

L'ensemble des traitements des données sensibles est effectué dans le cadre de systèmes d'information. « Un système d'information (SI) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information dans un environnement donné. » [4] Il s'agit de l'objet principal de cet article. On ne peut pas parler de données sensibles sans aborder le principe du système qui met en mémoire toutes ces données. Le système d'information peut sécuriser comme rendre l'information vulnérable en fonction des technologies déployées et des garanties qu'il peut apporter. La notion de gestion des données est intimement liée à ce système.

Le recours à l'utilisation de systèmes d'information pour l'optimisation de la réalisation des missions des entreprises et des administrations est devenu nécessaire. Face au volume croissant des informations à traiter et face à l'extension du besoin de communication, les outils mis à disposition évoluent. Le traitement dans le cas d'un système d'information désigne l'ensemble des fonctions de l'outil. La sécurité du système d'information correspond à l'état de protection face aux menaces et risques qui pourraient survenir. Ceci vise à assurer la confidentialité en limitant l'accès aux seules personnes autorisées et la disponibilité de l'information qui définit l'aptitude du système en terme d'horaire, de délais et de performance. Un troisième aspect est celui de l'intégrité qui garantie que l'information n'est pas modifiée de manière involontaire ou illégitime et que la traçabilité est assurée dans tous les cas de figure. En matière de sécurisation des systèmes d'information c'est la norme l'ISO/CEI 27005:2008 puis ISO/IEC 27005:2011 [5] qui définit les cadres et obligations. L'ISO, qui est l'Organisation internationale de la normalisation, a publié cette première norme le 4 juin 2008 qui est devenu un standard international en terme de Système de Management des risques liés à la Sécurité de l'information. En terme de moyens, les données peuvent être cryptées, sécurisées et transportées par des moyens sécurisés comme le SFTP qui permet un transfert sécurisé entre deux entités de données sensibles. De nombreux prestataires proposent des solutions sécurisées de gestion de données : plateforme collaborative, entrepôt de données, certification des serveurs et des hébergements. Beaucoup de garanties sont proposées en France comme ailleurs et à ce titre nous pouvons aussi citer des progiciels de type ERP - CRM (AGE, SAP, Enablon, Mercator) qui proposent des outils de sécurisation des systèmes d'information.

L'état de protection des données en garanti la confidentialité, la disponibilité et l'intégrité. En France, c'est la norme ISO qui détermine les normes de sécurisation à garantir des systèmes d'information pour traiter des données sensibles. Nous allons aborder, dans une nouvelle partie, l'exemple de la certification P.S.F. délivrée par la CSSF (Commission de Surveillance du Secteur Financier) au Luxembourg.

Comment sont alors garanties la confidentialité des données sensibles ? Quelles sont les classifications des opérateurs et les garanties apportées pour en garantir l'état lors de leur externalisation à des fins d'impression?

III. ETUDE SUR L'EXTERNALISATION DE L'IMPRESSION DES DONNEES SENSIBLES BANCAIRES

Sur la base d'une consultation faite auprès de plusieurs prestataires P.S.F. (dans le cadre d'une clause de confidentialité les noms des entreprises en question ne seront pas communiqués) au Grand Duché du Luxembourg, nous montrerons comment les données sensibles sont traitées et les services qui sont associés dans la cadre de la certification P.S.F - agent de communication. Les lois luxembourgeoises imposent aux entreprises qui travaillent pour le secteur financier d'obtenir le statut P.S.F. (Professionnel du Secteur Financier). Ce statut se décline en trois parties : P.S.F pour les entreprises d'investissement, entreprises dites spécialisées et entreprises de services. Selon la définition donnée par « Luxembourg for Finance », une société qui postule à la certification P.S.F est une entreprise qui fournit des services d'externalisation à des organismes de type établissement de crédit, de gestion de fonds, de fonds de pension, d'assurance entreprise ou de réassurance, l'UCI (Undertaking For Collective Investment), ou d'une autre P.S.F. comme une société d'investissement. Cela comprend les services relatifs à l'infrastructure des technologies de l'information et des services de sécurité, les systèmes de sauvegarde des données et l'archivage. Pour avoir la possibilité de travailler pour ce secteur, il faut obtenir au préalable la certification qui garantie que l'entreprise opère sur le même régime réglementaire que les intermédiaires financiers eux-mêmes. La loi couvre de nombreuses activités et une entreprise peut être certifiée dans plusieurs domaines. Il existe quatre catégories de certification :

- **Les agents de communication** dont les imprimeurs font partie : la production, la maintenance, la destruction, la distribution et l'archivage de déclarations des investisseurs et des clients;
- **Les agents administratifs** : s'engager dans la prestation de service d'administration faisant partie intégrante des activités commerciales de la P.S.F.;
- **Les opérateurs primaires de systèmes informatiques** : responsables de l'exploitation des systèmes informatiques qui génèrent des comptes et les états financiers qui font partie des systèmes informatiques de la P.S.F. ;
- **Les systèmes informatiques secondaires et opérateurs de réseaux de communication :** responsable de l'exploitation des systèmes autres que ceux qui génèrent les comptes et les états financiers et de la communication des réseaux qui font partie des systèmes informatiques de la P.S.F. Ceci inclut le traitement ou transfert de données stockées dans les systèmes informatiques.

Au delà de la classification des entreprises en fonction du type d'activité, la certification P.S.F. garantie un niveau d'exigences dans la cas de l'outsourcing et en ce qui nous concerne de l'impression des données sensibles.

L'impression des données est un processus à risque. Il

convient d'apporter des garanties quelles soient techniques, humaines ou bien encore logistiques.

A. Impression des données sensibles : contraintes

Les imprimeurs qui souhaitent travailler pour ces entreprises sont confrontés à la nécessité de cette certification. Ils sont concernés en tant que P.S.F – agent de communication. Ils doivent fournir les garanties suffisantes pour veiller au bon déroulement du traitement et de l'utilisation des données confiées. Certaines banques pour des raisons d'habitudes ou de défiance, gèrent en interne les impressions et les mises sous plis de leurs documents clients. Le recours à l'externalisation ou le phénomène du « outsourcing » dans le domaine peut s'expliquer par la mise en place de procédures dont la politique est de réduire les coûts et d'optimiser la rentabilité des salariés à des missions plus génératrices de bénéfices pour l'entreprise. On parle ici de « Facility Management ». Il a été défini par Relgerchot et Becker [8] comme étant « souvent défini comme la gestion intégrale (planification et contrôle) des logements, des services et des moyens qui contribuent à la réalisation efficace, flexible et créative des objectifs de l'organisation d'un cadre changeant ». Les leaders dans le domaine sont trois entreprises au profil très différent. Lors d'une consultation de ces trois entreprises, nous avons pu constater trois niveaux d'intégration avec des similitudes et des différences importantes de gestion des données à caractères confidentielles sur lesquelles nous reviendrons un peu plus tard dans cet article. Pour les imprimeurs ce label garantit trois aspects du prestataire la sécurité, les solutions déployées et les aspects administratifs basée sur l'approche de la gestion des risques (selon la motion de la CSSF 12/544 [6]). Pour les imprimeurs ce label garantit trois aspects du prestataire :

- **Sécurité :** cela peut concerner l'immobilier, les locaux, l'informatique mais aussi l'identification des personnes travaillant sur site que se soit du personnel interne ou externe.
- **Les solutions déployées :** les aspects traités ici sont la traçabilité des informations, les procédures opérationnelles ainsi que la gouvernance.
- **Les aspects administratifs :** que cela concerne la réalisation d'audit interne ou externe, les reporting règlementaires ou la gestion du risque basé sur l'approche (selon la notion de la CSSF 12/544).

Ils peuvent intervenir dans différents types d'opérations comme l'impression et la mise sous pli d'extraits de compte, des avis d'opérations, de rapport trimestriel ou bien encore dans la mise en place de mailings personnalisés. Cela peut concerner des banques de gestion ou d'investissement ou des banques privées. Au travers de cette étude de cas, nous allons étudier l'approche mais aussi le processus fonctionnel de dématérialisation des données sensibles qui permettent au prestataire de matérialiser sous forme papier les données brutes ou les documents transmis par les banques. Les trois prestataires rencontrés proposent des garanties de niveaux différenciés. Toutefois, tous proposent l'enrichissement des documents ou des données sources pour en assurer la traçabilité et déploient des moyens pour assurer la sécurité et l'intégrité. Au travers du schéma relationnel de communication entre les différents acteurs, nous irons au delà des solutions proposées par ces entreprises et des garanties de cette norme les évolutions de services et les perspectives associées.

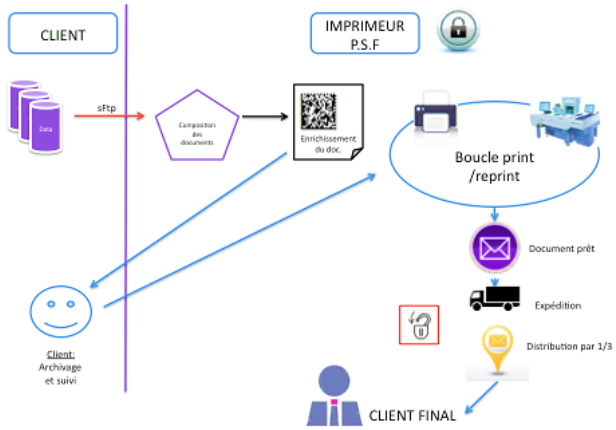

Fig. 1 : Approche fonctionnelle du traitement en impression P.S.F.

L'approche fonctionnelle soulève un certain nombre de questions. L'étude du processus d'impression des données sensibles de type relevé de comptes (*statement account*) ou tout autre communication à destination du client est complexe. L'ensemble de la chaîne doit être certifié jusqu'au dépôt postal. L'étude des principes de dématérialisation permet d'apporter des réponses complémentaires.

B. Processus d'impression : cas d'une banque privée

Les données arrivent à l'imprimeur sous plusieurs formes. Cela peut être des données brutes, des PDF, des données csv, fichiers Excel… En fonction du type de données un système de gestion de l'information est mis en place plus ou moins complexe selon des éléments reçus. Le transfert entre la banque et l'imprimeur peut se faire par plusieurs moyens : SFTP, mise en place d'un serveur de la banque au sein des locaux ou tout autre moyen qui pourrait être imposé par le responsable gestion des risques au sein de la banque.

Les documents sont ensuite créés selon les templates du client. À noter que les impressions peuvent se faire selon plusieurs méthodes : impression sur papier à entête pré imprimé, impression intégrale du support ce dernier à un coût plus élevé que la mis en place de templates sur papier pré-imprimé, en quadrichromie ou noir.

La traçabilité des documents

Une fois ces documents créés, ils sont ensuite enrichis pour en garantir la traçabilité tout au long du processus de traitement. Cela peut être mise en place par plusieurs procédés : datamatrix Code, QR Code ou bien encore code barre.

Fig.2 : Les procédés de traçabilité des documents

Une fois enrichi de cet outil de traçabilité, le fichier/ le document peut être renvoyé au client pour archivage en interne ou l'imprimeur peut proposer des solutions d'archivage sécurisé répondant aux normes P.S.F. À tout moment le client peut voir l'état d'avancement des données à caractère confidentiel qu'il a confié à l'imprimeur. Il existe, dans deux cas sur trois des prestataires rencontrés, la possibilité de suivre via un web service ces services les reporting (KPI), les erreurs et les anomalies du traitement, le nombre de documents imprimés et le nombre de documents en sortie de processus. À ce moment, le document rentre dans la « boucle d'impression » et de mise sous pli.

En cas d'incident pendant ce processus plusieurs méthodes peuvent intervenir en fonction des prestataires. Dans le cas présent, aucune intervention humaine n'est réalisée. Le nombre de documents et d'enveloppes en sortie doit être conforme à l'ordre d'impression. Dans le cas contraire les documents et enveloppes bloquent le système et l'ensemble et retraité jusqu'à obtention d'un taux de 0% d'erreur. Dans d'autres imprimeries P.S.F. d'autres solutions sont déployées : l'enveloppe ou le(s) document(s) concernés sont sortis de la chaîne. Grâce à leur traçabilité ils sont identifiés puis retraités. Ils sont soit remis en début de chaîne automatisée puis mis sous pli individuellement de manière automatique si le nombre d'erreur est suffisant pour lancer la machine à mise sous pli ou de manière manuelle si le nombre est insuffisant. L'ensemble du processus doit être réalisé dans un local sécurisé. Lors des visites sur site, nous remarquons différents degrés de sécurisation de ces locaux. De manière générale les locaux sont munis d'un système de vidéo surveillance et de contrôle aux entrées et sorties. Un registre des visiteurs est tenu à jour. Dans deux des trois entreprises visitées le site P.S.F. se situe au rendez de chaussée et deux sur trois ont des vitres opaques. Dans deux cas sur trois, ces chaînes P.S.F. sont localisées sur deux sites distincts et séparés de plusieurs kilomètres ce qui garanti la non rupture de la chaîne de production en cas de problèmes rencontrés lors du traitement. Enfin, dans deux cas sur trois la chaîne d'impression est exclusivement P.S.F. Pour un des imprimeurs, nous avons constaté que certains documents non sensibles se trouvaient sur la chaîne de production notamment lors de la phase de façonnage.

Une fois imprimé et mis sous pli, les documents matérialisés sont confiés à l'organisme de poste. Ils sont déposés au bureau de poste par l'intermédiaire de sociétés de transport sécurisé de type « Brinks ». Au Luxembourg, le service postal se nomme les P&T. Les documents peuvent être envoyés selon les volontés du client en courrier simple avec l'utilisation ou non de leur contrat de poste ce qui les amènera à gérer ou non les retours de courrier confidentiel ou à en laisser la gestion à l'imprimeur si celui ci utilise son numéro d'identification. De plus, les plis peuvent être déposés dans les postes voisines à savoir française, allemande ou belge. Le transport entre la salle sécurisée de l'imprimeur et la poste peut être effectué de différentes manières. Il est à savoir qu'il n'existe pas de traitement particulier de ce type de courrier une fois arrivé dans les services postaux. La garantie de confidentialité est assurée jusqu'à la porte de l'imprimeur voir du coursier qui livre aux services postaux. Ceci nous amène donc à souligner le fait qu'une fois confié aux services des P&T l'anonymisation des envois et l'une des seule précaution prise pour garantir la confidentialité des données. En cas de déchirage ou de perte volontaire ou non, d'erreurs lors du dépôt, les données sensibles peuvent se retrouver dans les mains de n'importe quel individu. Le document composé de données confidentielles est donc vulnérable pendant la distribution. De plus, nous pouvons nous interroger sur l'avenir et l'évolution de ce statut au vue des annonces de levé du secret bancaire au Luxembourg. En ce qui concerne la destruction des documents non utilisés ou des calages réalisés pour les machine d'impression, il doit être garanti au client que ces documents seront détruits et non utilisables en sortie de chaîne. Nous allons, dans le panel consulté, de l'élimination par destructeur professionnel en interne puis mise dans les poubelles traditionnelles à la destruction garantie de niveau 5 à savoir la réduction en paillettes en interne, la mise sous des containers sécurisés et la possibilité de destruction par un prestataire spécialisé garantissant un niveau optimal en terme de sécurité.

Il existe des points d'amélioration qu'il convient d'énoncer et d'exploiter. Ils peuvent permettre d'optimiser le processus.

C. Optimisation du processus d'impression

À la fin du processus, certains contrats d'impression P.S.F vont jusqu'à garantir l'effacement des données dans un temps défini avec le client. Au niveau de la gestion des systèmes d'information, il existe plusieurs systèmes qui garantissent la sécurisation des données. Il existe par exemple un système d'implémentation de V-Lan séparant les environnements clients, la mise en place du transfert fichiers via connexion sécurisée (SFTP), la présence de deux firewalls de protection du réseau informatique, une politique de mots de passe complexes, une cryptage systématique des fichiers de production, et enfin la séparation des environnements de test indispensables à la mise en place de toute impression P.S.F. de l'environnement de production opérationnel. La gestion de « la séparation clients « et les procédures d'effacement des fichiers complexes peuvent faire partie aussi des garanties

données aux clients. Dans ce domaine, nous avons pu remarquer la présence de trois leaders sur le marché qui pour l'un d'entre eux revendique l'obtention de parts de marché de la société des P&T.

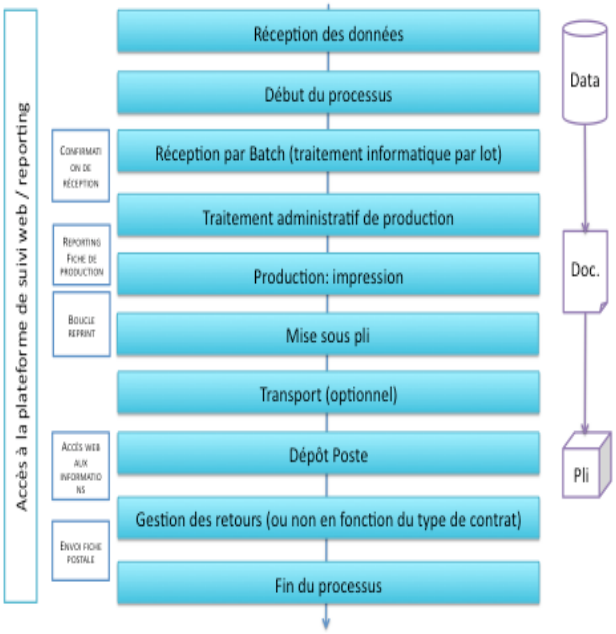

Fig.3: le processus fonctionnel du traitement des données à caractère confidentiel P.S.F.

Le rôle de la CSSF (Commission de Surveillance du Secteur Financier) :

La CSSF (Commission de Surveillance du Secteur Financier) est l'autorité de surveillance et d'attribution des autorisations P.S.F. Ce statut a été introduit au Luxembourg par la loi du 2 août 2003 qui a amendé la loi du 5 avril 1993 relative au secteur financier (article 12-23 du 5 avril 1993 et 29.1 – 29.4 de la même loi – [10]).

La demande d'autorisation et de certification doit être faite par une identité légale en mentionnant les informations suivantes :

- La publication de la création de l'entreprise au Journal Officiel qui est publique au Luxembourg et consultable en ligne.
- Le descriptif des activités concernées de l'entreprise ce qui est appelé Memorandum.
- Le nom des personnes en charge de l'entreprise (Conseil d'administration, dirigeant(s), …) et décisionnaires ainsi que le pourcentage de capitaux détenu par chacun d'entre eux.
- L'organigramme complet de la société doit être fournit.
- Les noms, Curriculum Vitae, relevé de police, et déclaration personnelle sur l'honneur de chaque membre de l'équipe et de chaque chef de service qui sera en charge ou membre des projets sensibles.
- Le nom de la société qui est en charge de l'audit externe annuel.
- Le nom de l'auditeur interne.
- La mise à disposition d'un budget prévisionnel pour les trois années à venir.
- Le détail des ressources humaines et matérielles qui vont être mises à contribution au Luxembourg.
- Les procédures déployées pour lutter contre le blanchiment d'argent et de garantir de connaissances de ses clients « Know Your Customer » (KYC).

IV. Conclusion et perspectives

Un tel pays spécialisé dans le domaine bancaire le Luxembourg, a commencé à initier des solutions de sécurisation de ses données dans les années 90.

Pays libéral, il est question d'optimisation des ressources humaines internes et en ce sens certaines sociétés notamment dans le domaine bancaire cherchent à externaliser tout ou partie de leurs activités principalement sur le territoire luxembourgeois.

Les coûts de développement de solutions en interne sont très élevées et sont réservées à des entreprises qui font partie des « Big 4 » (sociétés cotées en bourse sur la place financière luxembourgeoise). Il est parfois surprenant de voir comment étaient gérées en interne les missions externalisées : manque de sécurisation et outils peu ou pas adaptés au traitement de données confidentielles. De manière très large, le Luxembourg ouvre ses portes depuis seulement quelques années à une concurrence de plus en plus féroce du monde entier. Ce pays n'était pas prêt et encore moins formé à anticiper ces aspects. Des problématiques particulières liées à la composition même du personnel de ses entités (personnel étranger provenant de la France, de la Belgique et de l'Allemagne mais aussi de tous les pays de l'Union européenne et du monde entier). De ce fait, les « fuites » peuvent être très importantes et causer beaucoup de dégâts. Un autre aspect à la gestion en interne de ce type de données est le taux d'erreur. Un personnel non attitré à ce type de traitement qui peut avoir plusieurs activités en même temps ou qui peut ne pas être formé ou bien encore le manque de temps ou de moyens pour réaliser ses tâches. Le taux d'erreur pousse souvent les entreprises (bancaires) à externaliser pour aboutir à de meilleurs résultats.

Les imprimeurs dont il a été question dans ce cas d'étude ont pour deux d'entre eux fournis les arguments nécessaires pour convaincre de leur fiabilité qui semble à la fois nécessaire mais impérative. Une réserve toutefois est à apporter quant à l'expédition des plis. Certains imprimeurs P.S.F nous ont indiqué passer par des transporteurs comme DHL ou des petits transporteurs locaux, d'autres par des systèmes identiques à ceux des convoyeurs de fonds.

Pourquoi ne pas pousser ce niveau de sécurisation à la distribution incluse à ce système sécurisé du début à la fin ? Le recommandé ou un autre type d'envoi ne générant pas trop de surcoût pour les banques.

Diffusion des données confidentielles [11]

Un des prestataires rencontrés, nous a présenté les solutions proposées pour diffuser de l'information confidentielles aux clients de notre banque privée en dehors de l'impression traditionnelle. Ils ont développés un certain nombre d'outils en phase avec les évolutions du métier d'imprimeur. Face aux

incertitudes et au constat de diminution du nombre de documents imprimés certains imprimeurs se diversifient dores et déjà. Phénomène de mode, ou le banquier devient opérateur mobile et assureur, l'imprimeur dont il est question s'est associé avec une société d'informatique qui propose des solutions clefs en mains pour la communication directe vers le client de ses données à caractère confidentiel et sensible avec la garantie d'un hébergement luxembourgeois.

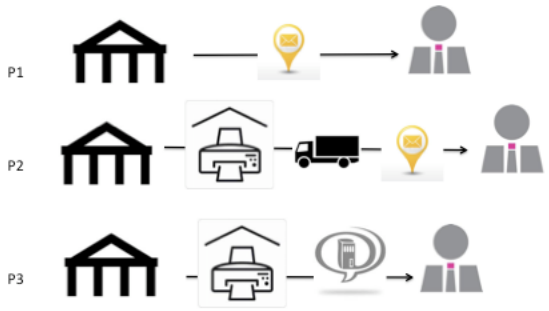

Fig.4 : Schéma de communication associé aux méthodologies de traitement

Schéma relationnel de communication des trois processus décrits :

P1 processus initial: Banque - P&T - Client

P2 Processus impression: Banque - Imprimeur - (transporteur) - P&T- Client

P3 Processus dématérialisé: Banque - Imprimeur - Prestataire IT - Client

Les évolutions des usages et des besoins ont permis le développement de nouvelles solutions basées sur l'approche dématérialisée.

Peut on parler d'une optimisation de la sécurité des données par la dématérialisation ?

Le premier développement proposé est la mise à disposition d'une plateforme web-based en mode S.a.a.S (Software as service). Cette dernière est proposée avec une gestion de l'hébergement en externe. Ce dernier peut être assuré au Luxembourg par une société de service qui garantie les aspects P.S.F dans son Datacenter [12]. Cela permet aussi une haute disponibilité de stockage et une haute disponibilité de la bande passante. Ainsi sont garantis la diffusion et l'accès en un temps optimal au téléchargement. De plus, la société met à disposition un portail d'accès avec identification du client qui propose l'ensemble de solutions proposées et pour lequel le client peut choisir des options opérationnelles [13]. Cette dernière propose aussi des fonctionnalités complémentaires comme la mise à disposition d'outils qui permettent aux banques d'envoyer directement à leurs client des Newsletter créées à partir de cet outil, de générer des e-mailing, des e-news et enfin des applications pour les Smartphones et les tablettes tactiles adaptées pour leurs clients notamment pour les services de banque en ligne (web banking). De ces fonctionnalités, les clients peuvent ensuite faire une évaluation de la portée de leurs actions par l'accès aux statistiques de leurs opérations de e-publishing (publication en ligne au travers du nombre de téléchargements et la traçabilité qui peuvent être analysés.

BIBLIOGRAPHIE

[1]- Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classées de défense, Disposition interministérielle 901 .[URL visited 23/02/14]. http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_2007.pdf

[2]- Instruction générale interministerielle sur le protection du secret de la Défense nationale, Disposition interministérielle 1 300 .[URL visited 23/02/14]. http://www.ssi.gouv.fr/archive/fr/reglementation/igi1300.pdf

[3]- Loi informatique et liberté de 1978.[URL visited 23/02/14]. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20080609

[4]- De Courcy R., Les systèmes d'information en réadaptation, Québec, Réseau international CIDIH et facteurs environnementaux, 1992, no 5 vol. 1-2 P. 7-10

[5]- ISO/IEC 27005:2011- Technologie de l'information- techniques de sécurité- gestion des risques liés à la sécurité de l'information.

[6]- Motion de la CSSF 12/544.[URL visited 23/02/14]. http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf12_544.pdf

[7]- Carole Henry Optimisation de processus de collecte et d'exploitation d'informations sensibles: cadre d'étude du renseignement intérieur, ISKO Maghreb 2013.[URL visited 23/04/14].http://hal.archives-ouvertes.fr/hal-00933040

[8]- Relgerchot et Becker, Becker, F. 1990. The Total Workplace: Facilities Management and the Elastic Organiazation. Van Nostrand Reinhold, New York, USA.[URL visited 23/02/14].http://www.journal.au.edu/au_techno/2002/jul2002/article4.pdf

[9]- Les données personnelles. Qu'est ce qu'une donnée sensible?..[URL visited 30/03/14].(http://www.donneespersonnelles.fr/qu-est-ce-qu-une-donnee-sensible)

[10]-PWC.Loi du 5 avril 1993.[URL visited 30/03/14]. http://www.pwc.lu/en_LU/lu/banking/docs/pwc-banking-050493-fr.pdf

[11]-P&T.[URL visited 25/04/14]. http://www.netcore.lu/Solutions/DataCenter/Data

[12]-Paperjam.[URL visited 25/04/14]. http://www.paperjam.lu/article/fr/profession-diffuseur-d-information

[13]-Dataline.[URL visited 25/04/14].http://www.dataline.eu/fr/imprimerie-faber-321.htm

[14]- Décret N°81-514 du 12 mai 1981. Art.2. Journal Officiel.Organisation de la protection des secrets et des informations concernant la defense nationale et la sûreté de l'Etat. .[URL visited 13/09/14]. http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19810515&pageDebut=01427&pageFin=&pageCourante=01427

[15]-Marking classified National Security Information. ISOO-2010. [URL visited 13/09/14]- http://www.archives.gov/isoo/training/marking-booklet.pdf