Commission nationale de l'informatique et des libertés

Délibération nº 2013-270 du 19 septembre 2013 portant recommandation relative aux services dits de « coffre-fort numérique ou électronique » destinés aux particuliers

NOR : *CNIX1324552X*

La Commission nationale de l'informatique et des libertés,

Vu la convention nº 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/47/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 sur la réutilisation des informations du secteur public ;

Vu la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11 ;

Vu le décret nº 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu M. Jean François CARREZ, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La Commission nationale de l'informatique et des libertés constate que la dématérialisation de documents, après être entrée dans les mœurs du monde de l'entreprise, se développe à présent auprès des particuliers. La montée en puissance du commerce électronique ou des téléservices incite en effet ces derniers à diffuser, recevoir ou stocker plus fréquemment des informations les concernant sous forme électronique.

La centralisation de documents dématérialisés en un lieu unique est par nature risquée et pose des problèmes spécifiques au regard de la loi du 6 janvier 1978 modifiée, qu'il s'agisse de la destruction des données, de leur perte, de leur altération ou encore de leur divulgation à des tiers non autorisés.

A l'issue d'une concertation avec certains des principaux acteurs concernés, la Commission nationale de l'informatique et des libertés a souhaité préciser sa position vis-à-vis des services dits de « coffre-fort numérique ou électronique ».

1. **Définition**

Un espace de stockage numérique est un service qui a pour objet de conserver des documents dématérialisés sur un support informatique.

La commission considère que le terme coffre-fort numérique ou coffre-fort électronique doit être réservé à une forme spécifique d'espace de stockage numérique, dont **l'accès est limité à son seul utilisateur et aux personnes physiques spécialement mandatées par ce dernier.**

La commission estime que les services dits de coffre-fort numérique doivent garantir l'intégrité, la disponibilité et la confidentialité des données stockées et impliquer la mise en œuvre des mesures de sécurité décrites dans la présente recommandation.

Le fournisseur du service ne doit pas être techniquement en mesure d'accéder au contenu d'un coffre-fort, ni à ses éventuelles sauvegardes, sans le consentement exprès de l'utilisateur concerné.

La commission estime qu'un service qui ne répondrait pas à ces critères et aux mesures décrites ci-après est un simple espace ou service de stockage numérique au sens de la présente recommandation.

2. **Applicabilité de la loi du 6 janvier 1978 modifiée**

Un service de coffre-fort numérique est un traitement automatisé de données à caractère personnel. D'une part, sa gestion repose sur des opérations informatisées. D'autre part, le contenu d'un espace de stockage est par nature lié à une personne physique identifiable.

La loi du 6 janvier 1978 modifiée est ainsi applicable à l'ensemble des services de coffre-fort numérique proposés aux particuliers par des sociétés établies sur le territoire français.

S'agissant des sociétés établies en dehors du territoire de l'Union européenne et proposant de tels services, la loi du 6 janvier 1978 modifiée leur est également opposable dès lors qu'elles utilisent des moyens de traitement en France.

La loi du 6 janvier 1978 modifiée n'est en revanche pas applicable à un espace de stockage numérique de documents créé par un particulier sur un support matériel lui appartenant, dès lors que seules des données le concernant y sont conservées pour son usage personnel.

3. **Formalités préalables à la mise en œuvre d'un service de coffre-fort numérique**

Le fournisseur d'un service de coffre-fort numérique détermine les moyens et les finalités dans la mise en œuvre du traitement. Il est ainsi, à la lecture de l'article 3-I de la loi du 6 janvier 1978 modifiée, le responsable du traitement et il lui appartient en cette qualité d'accomplir les formalités auprès des services de la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du service.

Un service de coffre-fort numérique ou électronique doit faire l'objet, avant sa mise en œuvre, d'une déclaration normale auprès des services de la Commission nationale de l'informatique et des libertés.

La déclaration doit préciser, notamment, les catégories de données à caractère personnel traitées par le prestataire pour assurer son service (données d'identification des utilisateurs et données de connexion).

En revanche, les catégories de données stockées par les utilisateurs n'ont pas à être mentionnées dans la déclaration. En effet, il est impossible de déterminer à l'avance le type de documents qu'un utilisateur décidera de stocker dans son espace personnel, d'une part, et il est techniquement impossible de le savoir *a posteriori* puisque, par définition, le contenu d'un coffre-fort numérique ne doit pouvoir être consulté que par l'utilisateur concerné et les personnes mandatées par ce dernier, d'autre part.

La Commission nationale de l'informatique et des libertés estime que les opérations de récupération automatique de documents dématérialisés ne sont pas des interconnexions de fichiers issus de traitements dont les finalités principales sont différentes, dès lors que les documents ne sont pas utilisés par le fournisseur du service mais seulement introduits à un coffre-fort numérique.

En application de l'article 69 de la loi du 6 janvier 1978 modifiée, si les données stockées par les utilisateurs d'un service de coffre-fort numérique doivent être transférées en dehors de l'Union européenne par le prestataire, ce dernier doit obtenir une autorisation préalable de la Commission nationale de l'informatique et des libertés.

Recommande :

S'agissant des donnés traitées :

Un fournisseur de service de coffre-fort numérique de documents est amené à traiter au minimum des données permettant d'identifier de façon certaine les utilisateurs, d'une part, ainsi que les données de connexion nécessaires au fonctionnement de son service, d'autre part. Ces catégories de données doivent figurer dans la déclaration du traitement accomplie auprès de la Commission nationale de l'informatique et des libertés.

La Commission nationale de l'informatique et des libertés rappelle que le traitement de certaines catégories de données est, selon les cas, interdit ou réglementé.

Ainsi, le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, c'est-à-dire le numéro de sécurité sociale, ne peut être utilisé pour le routage d'un document dématérialisé vers un coffre-fort numérique, y compris lorsqu'il s'agit de router des bulletins de paye. Les utilisateurs peuvent néanmoins stocker leurs bulletins de paye dans leurs coffres-forts électroniques.

Par ailleurs, l'hébergement de données de santé est soumis à un régime juridique spécifique. En effet, en application de l'article L. 1111-8 du code de la santé publique, les hébergeurs de données de santé doivent obtenir un agrément ministériel spécifique. La Commission nationale de l'informatique et des libertés considère, par conséquent, que les fournisseurs de coffres-forts numériques ne peuvent proposer à leurs utilisateurs de stocker des données relatives à la santé s'ils ne sont pas agréés à cet effet. Elle en déduit que la mise en avant du stockage de telles données ou son organisation, y compris la simple création par défaut d'un dossier « santé » par le fournisseur, nécessite impérativement l'obtention préalable de l'agrément ministériel précité. Les fournisseurs non agréés, quant à eux, doivent déconseiller à leurs utilisateurs de stocker des données relatives à la santé.

S'agissant des destinataires :

Lorsqu'un service de stockage numérique est présenté comme un service de coffre-fort numérique, les documents stockés ne doivent être consultables que par l'utilisateur concerné et les personnes spécialement mandatées par ce dernier.

Le contenu d'un coffre-fort numérique doit ainsi être protégé par des mesures techniques les rendant incompréhensibles aux tiers non autorisés.

S'agissant des durées de conservation :

Lorsqu'un utilisateur souhaite supprimer l'un des documents de son espace personnel, cette opération doit être immédiatement prise en compte.

Les copies répliquées en ligne du document supprimé doivent également être supprimées sans délai. Les éventuelles sauvegardes dans lesquelles peuvent figurer ces données ne doivent pas quant à elles être conservées au-delà d'un mois.

Il est toutefois possible de conserver brièvement un document qu'un utilisateur souhaite supprimer, notamment afin de détecter une éventuelle anomalie quant à l'utilisation de son espace personnel, ou de lui permettre de revenir sur sa décision en cas de mauvaise manipulation.

Lorsqu'un service de stockage numérique est présenté comme un service de coffre-fort numérique, le fournisseur du service s'engage quant à la pérennité du stockage. Par conséquent, la fermeture de ce type de service nécessite d'en informer les utilisateurs suffisamment en avance afin de leur laisser le temps nécessaire pour récupérer les documents stockés.

S'agissant de l'information des personnes :

De façon générale, en application de l'article 32 de la loi du 6 janvier 1978 modifiée, les personnes concernées par un traitement de données à caractère personnel doivent être notamment informées de l'identité du responsable du service, de la finalité poursuivie, des destinataires des données, des éventuelles transferts de données à destination d'un pays non membre de l'Union européenne ainsi que de l'existence et des modalités d'exercice des droits d'accès, de rectification et d'opposition.

Les utilisateurs de coffres-forts numériques doivent, par conséquent, être clairement informés du type d'espace mis à leur disposition et de ses conditions d'utilisation.

Par ailleurs, lorsque que le fournisseur propose à ses utilisateurs un service de récupération de documents auprès de services tiers, basé sur la collecte des identifiants et mots de passe de l'utilisateur pour se connecter en leur nom à ces services tiers, il doit informer ses utilisateurs quant aux conséquences pouvant résulter de la collecte de leurs identifiants et mots de passe. En effet, une telle collecte peut constituer une violation des conditions générales d'utilisation de ces services tiers et des conséquences dommageables peuvent en résulter, telles que la perte du bénéfice d'une garantie ou d'une assurance.

La Commission nationale de l'informatique et des libertés recommande ainsi que les fournisseurs d'espaces de stockage numérique élaborent des solutions techniques permettant d'offrir des services de récupération de documents dématérialisés sans procéder à la collecte d'informations confidentielles.

S'agissant des mesures de sécurité :

– le fournisseur d'un service de coffre-fort numérique ne doit pas être en mesure d'accéder aux données ou de les réutiliser. Des mesures techniques doivent être mises en place pour rendre les données incompréhensibles aux tiers non mandatés par l'utilisateur ;
– les données doivent être chiffrées avec une clef, maîtrisée uniquement par l'utilisateur, conforme aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques éditées par l'Agence nationale de sécurité des systèmes d'information (ANSSI) dans son référentiel général de sécurité à l'annexe B1 ;
– lorsqu'un coffre-fort numérique a vocation à conserver des données à long terme, une copie de sauvegarde de la clef de déchiffrement doit être confiée à un tiers de confiance, afin de permettre à l'utilisateur d'accéder à ses données en cas de perte de sa clef. Toute utilisation d'une sauvegarde de la clef de déchiffrement doit faire l'objet d'une traçabilité et d'une information de l'utilisateur concerné ;
– lorsqu'un coffre-fort numérique a vocation à conserver des données à long terme, le fournisseur du service doit prévoir une évolution de la taille des clefs et des algorithmes utilisés afin de garantir la confidentialité des données stockées dans le futur ;
– tous les transferts d'information vers et depuis un coffre-fort numérique doivent être chiffrés lorsqu'ils sont réalisés par un canal de communication non sécurisé ;
– les fournisseurs doivent utiliser dans la mesure du possible des produits cryptographiques certifiés ou qualifiés par l'Agence nationale de sécurité des systèmes d'information (ANSSI) ;
– les fournisseurs doivent communiquer auprès de leur clients sur les mécanismes de chiffrement utilisés de la façon la plus transparente possible ;
– les fournisseurs doivent utiliser des mécanismes d'authentification robustes, de préférence des mécanismes d'authentification forte (mots de passe à usage unique, envoi de codes par SMS...) et respecter les recommandations de la Commission nationale de l'informatique et des libertés dans ce domaine. En cas d'utilisation de mots de passe, des mécanismes réduisant les risques liés aux choix de mots de passe faibles doivent être mis en place ;
– les fournisseurs doivent mettre en place des mesures visant à garantir l'intégrité et la disponibilité des données (centre de stockage redondant, sauvegardes régulières...) et apporter des garanties en termes d'indemnisation des personnes en cas d'ineffectivité de ces mesures ;
– les fournisseurs doivent apporter des garanties fortes pour prévenir toute perte de données en cas de cessation d'activité ;
– les fournisseurs doivent rendre accessible, sans surcoût, un outil permettant aux utilisateurs de récupérer l'intégralité du contenu de leur coffre-fort de façon simple, sans manipulation complexe ou répétitive, et ce afin de faciliter le changement de fournisseur ;
– les fournisseurs ne doivent pas inciter les utilisateurs à leur confier leurs identifiants et mot de passe permettant d'accéder en ligne à des services de la société de l'information sans les avoir préalablement informés quant aux conséquences de cette collecte ;
– lorsqu'un coffre-fort numérique permet d'échanger des données avec des tiers, le fournisseur doit mettre en place des mécanismes d'authentification de ces tiers ;
– les fournisseurs doivent proposer des fonctionnalités de traçabilité permettant aux utilisateurs de visualiser l'activité récente sur leur coffre-fort numérique afin de détecter les éventuelles intrusions non souhaitées ;
– les fournisseurs doivent mettre en place des outils permettant de détecter et bloquer les connexions illégitimes aux coffre-fort numériques ;

– l'effacement d'un fichier par un utilisateur doit être immédiatement pris en compte. Les copies répliquées du document supprimé doivent également être supprimées sans délai. Les éventuelles sauvegardes ne doivent pas être conservées au-delà d'un mois, ce délai apparaissant suffisant pour pallier une mauvaise manipulation de l'utilisateur ou corriger une anomalie ;
– les fournisseurs doivent informer leurs utilisateurs sur les mécanismes techniques qu'ils mettent en œuvre afin de leur permettre de juger du niveau de sécurisation du service proposé ;
– les utilisateurs doivent être informés quant aux modalités de résiliation du service et de récupération des données stockées ;
– à défaut d'obtention d'une autorisation préalable de la Commission nationale de l'informatique et des libertés, les données collectées dans le cadre d'un service de coffre-fort numérique doivent rester sur le territoire de l'Union européenne ou sur le territoire d'un Etat non membre de l'Union européenne garantissant aux données un niveau de protection suffisant au sens de l'article 68 de la loi du 6 janvier 1978 modifiée susvisée.

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. Falque-Pierrotin