Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe

Lien Légifrance : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000035142502

Version consolidée

La Commission nationale de l'informatique et des libertés ;

Vu la convention n° 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 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 11, 34 et 35 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Après avoir entendu M. François PELLEGRINI, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;

Formule les observations suivantes :

En application de l'article 34 de la loi du 6 janvier 1978 modifiée, le responsable d'un traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De même, l'article 35 de la loi du 6 janvier 1978 modifiée prévoit que les sous-traitants et les personnes agissant sous l'autorité du responsable du traitement ou du sous-traitant, doivent présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34, ce qui ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

À cet égard, il ressort des échanges que la CNIL a avec les responsables de traitements dans le cadre de ses missions de conseil et de contrôle, tant *a priori* qu'*a posteriori*, que le moyen d'authentification actuellement le plus répandu dans le cadre du contrôle d'accès à une ressource numérique, est celui associant un identifiant à un mot de passe (secret).

Toutefois, la Commission a toujours considéré que d'autres moyens offrent davantage de sécurité, comme par exemple l'authentification à double facteur ou les certificats électroniques.

En outre, la multiplication des attaques informatiques, qui a entrainé la compromission de bases de données entières contenant notamment les mots de passe associés aux comptes des personnes concernées, a pour conséquence l'amélioration des connaissances des attaquants en matière de mots de passe.

Enfin, le fait que les utilisateurs emploient un même mot de passe pour se connecter à différents comptes en ligne renforce l'obligation pour les responsables de traitement de mettre en œuvre toutes mesures permettant d'assurer la sécurité des données à caractère personnel.

Dans ce contexte, et dans l'objectif d'apporter une plus grande confiance dans les services du numérique, il apparaît nécessaire que la Commission définisse les modalités techniques de cette méthode d'authentification, à même de garantir un niveau de sécurité adapté, et édicte des recommandations relatives aux mesures à mettre en œuvre, ainsi que les règles à respecter, quant à son utilisation.

À cet effet, la Commission a échangé tant avec ses homologues européens qu'avec des institutions et professionnels en charge de sécurité de l'information, afin de bâtir un référentiel technique apportant un niveau de sécurité minimal, cohérent avec les bonnes pratiques de sécurité et concrètement applicable.

Compte tenu de ces observations préalables, la Commission émet la recommandation suivante, qui vient préciser et appliquer les dispositions de la loi du 6 janvier 1978 modifiée, en particulier ses articles 34 et 35.

Afin de proposer aux professionnels des lignes directrices en matière de gestion des mots de passe, la CNIL adopte cette recommandation. Celle-ci vise à interpréter les dispositions législatives précitées et à éclairer les acteurs sur la mise en place de mesures concrètes permettant de garantir le respect de ces dispositions dans l'état de l'art.

I. Sur le champ d'application de la recommandation

La présente recommandation concerne l'ensemble des traitements de données à caractère personnel mis en œuvre par des personnes publiques ou privées ayant recours à l'authentification par mot de passe, à l'exception de ceux pour lesquels des dispositions législatives ou réglementaires spécifiques fixent des prescriptions techniques particulières.

La recommandation fixe des modalités techniques minimales relatives à une authentification basée sur des mots de passe. En particulier, elle précise les modalités relatives à la création du mot de passe et à la gestion du compte associé, à l'authentification, à la conservation, au changement et au renouvellement du mot de passe, et à la notification de violations de données à la personne.

Les risques spécifiques qu'un traitement de données à caractère personnel peut faire peser sur la vie privée des personnes concernées peuvent exiger des mesures plus rigoureuses pour préserver la sécurité des données, telles celles concernant la gestion des mots de passe des administrateurs informatiques ou le traitement de données sensibles.

II. Sur les modalités techniques

1. Création du mot de passe et blocage de compte

S'agissant des modalités de création d'un mot de passe requis pour l'authentification à un compte, la Commission considère que la taille minimale et la complexité de ce mot de passe doivent être imposées par le responsable de traitement. Elle recommande en outre que la personne concernée

par le traitement en soit préalablement informée par le responsable de traitement, ainsi que de la taille maximale du mot de passe supportée par le traitement.

Quatre cas sont possibles. Le premier impose des exigences fortes en termes de taille et de complexité du mot de passe. Pour les suivants, ces exigences sont moins fortes, du fait de l'existence de mesures compensatrices visant à assurer un niveau de sécurité équivalent.

Dans tous les cas, la Commission estime que le mot de passe ne doit jamais être communiqué à l'utilisateur en clair, notamment par courrier électronique.

Cas n° 1 – Mot de passe seul

Si l'authentification repose uniquement sur un identifiant et un mot de passe, la Commission considère que :

- la taille du mot de passe doit être au minimum de 12 caractères ; et
- le mot de passe doit comprendre des majuscules, des minuscules, des chiffres et des caractères spéciaux.

La robustesse de cette authentification repose exclusivement sur la qualité intrinsèque du mot de passe de l'utilisateur. Aussi, la Commission estime que le responsable de traitement se doit d'alerter l'utilisateur à ce sujet et, dans la mesure du possible, le conseiller dans la création de son mot de passe.

Cas n° 2 – Mot de passe et restriction d'accès au compte

Si l'authentification prévoit une restriction de l'accès au compte, la Commission considère que :

- la taille du mot de passe doit être au minimum de 8 caractères ; et
- le mot de passe doit au minimum comporter 3 des 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux) ; et
- l'authentification doit faire intervenir une restriction de l'accès au compte, qui doit prendre une ou plusieurs des formes suivantes :
    - une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; la Commission recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou
    - un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : captcha) ; et/ou
    - un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10.

Cas n° 3 – Mot de passe et information complémentaire

Si l'authentification comprend une information complémentaire, la Commission considère que :

- la taille du mot de passe doit être au minimum de 5 caractères ; et
- l'authentification doit faire intervenir une information complémentaire, qui peut prendre l'une des formes suivantes :

- une information communiquée en propre par le responsable de traitement ou la personne concernée. La Commission recommande que cette information ait une taille d'au moins 7 caractères et ne soit connue que de la personne et du responsable de traitement. Si cette information correspond à l'identifiant du compte, il est recommandé que ce dernier soit propre au service (dédié exclusivement), fourni par le responsable de traitement, et uniquement connu de la personne et du responsable de traitement ; et/ou
- tout paramètre technique ayant caractère d'unicité sur le terminal informatique utilisé par la personne (adresse IP, adresse MAC, *user agent*, etc.) pour lequel la personne a préalablement validé qu'il s'agissait d'un terminal de confiance (p. ex. : terminal non public) et qu'il peut à tout moment révoquer ; et
- une restriction de l'accès au compte doit être mise en œuvre, pouvant prendre la forme d'une ou plusieurs des modalités suivantes :
  - une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; la Commission recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou
  - un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : captcha) ; et/ou
  - un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 5.

Cas n° 4 – Mot de passe et matériel détenu par la personne

Si l'authentification s'appuie sur un matériel détenu par la personne, la Commission considère que :

- la taille du mot de passe doit être au minimum de 4 chiffres ; et
- l'authentification ne peut concerner qu'un dispositif matériel détenu en propre par la personne, à savoir uniquement les cartes SIM, cartes à puce et dispositifs contenant un certificat électronique déverrouillable par mot de passe (*token*) ; et
- un blocage du dispositif doit être mis en œuvre après un nombre d'authentifications échouées consécutives au plus égal à 3.

2. Modalités de l'authentification

S'agissant des modalités de l'authentification au compte, la Commission considère que la fonction d'authentification doit être sûre (c'est-à-dire qu'elle utilise un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue).

Lorsque l'authentification n'a pas lieu en local, la Commission recommande qu'une mesure de contrôle de l'identité du serveur d'authentification soit mise en œuvre au moyen d'un certificat d'authentification de serveur. De plus, il recommandé que le canal de communication entre le serveur authentifié et le client soit chiffré à l'aide d'une fonction de chiffrement sûre (c'est-à-dire mettant en œuvre un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue). La Commission recommande en outre que la sécurité des clés privées soit assurée.

3. *Modalités de conservation*

S'agissant des modalités de conservation, la Commission considère que le mot de passe ne doit jamais être stocké en clair. Elle recommande que tout mot de passe utile à la vérification de l'authentification et devant être stocké sur un serveur soit préalablement transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé.

4. *Modalités du renouvellement du mot de passe et de la notification à la personne*

La Commission recommande que le renouvellement du mot de passe soit systématique en cas de compromission de celui-ci.

Dans tous les cas, elle estime que le mot de passe ne doit jamais être communiqué à l'utilisateur en clair, notamment par courrier électronique.

Renouvellement périodique du mot de passe

La Commission recommande que le responsable de traitement veille à imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.

Elle recommande aussi que le responsable de traitement permette à la personne concernée de procéder elle-même au changement de son mot de passe. Dans ce cas, les règles afférentes à la création de mots de passe s'appliquent.

Renouvellement sur demande du mot de passe

À la demande de la personne concernée, par exemple en cas d'oubli, la Commission recommande que le responsable de traitement mette en œuvre une procédure de renouvellement du mot de passe, conformément à ce qui suit :

- lorsque ce renouvellement nécessite l'intervention d'un administrateur, la Commission estime que la procédure d'authentification doit imposer le changement du mot de passe attribué temporairement par l'administrateur à la première connexion de la personne ;
- lorsque ce renouvellement intervient de manière automatique :
    - la Commission considère que le mot de passe ne doit pas être transmis en clair à la personne ; il est recommandé que celle-ci soit redirigée vers une interface lui permettant de saisir un nouveau mot de passe ; la validité de la session de cette interface ne devrait pas excéder 24 heures, et ne pas permettre plus d'un seul renouvellement ; ou
    - si le renouvellement fait intervenir un ou plusieurs éléments supplémentaires (numéro de téléphone, adresse postale, etc.) :
        - la Commission considère que ces éléments ne doivent pas être conservés dans le même espace de stockage que l'élément de vérification du mot de passe ; sinon, il est recommandé qu'ils soient conservés sous forme chiffrée à l'aide d'un algorithme public réputé fort, et que la sécurité de la clé de chiffrement soit assurée ; et

- afin de prévenir les tentatives d'usurpation s'appuyant sur le changement de ces éléments, la Commission considère que la personne doit être immédiatement informée de leur changement.

Notification de violation à la personne concernée

La Commission recommande que le responsable de traitement notifie la personne concernée quand une violation de son mot de passe ou de données liées au renouvellement (p. ex. : adresse électronique) a été détectée, dans un délai n'excédant pas 72 heures depuis la constatation de la violation. La Commission estime que le responsable de traitement doit imposer dans ce cas le changement du mot de passe à la personne concernée lors de sa prochaine connexion, et recommande à la personne de veiller à changer ses mots de passe d'autres services dans l'hypothèse où elle aurait utilisé le même mot de passe pour ceux-ci.

III. Dispositions transitoires et finales

La présente délibération est publiée au *Journal officiel de la République Française*.

La Présidente

Isabelle FALQUE-PIERROTIN