Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2018-010 du 6 septembre 2018

Délibération de la formation restreinte n° SAN-2018-010 du 6 septembre 2018 prononçant une sanction pécuniaire à l'encontre de l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE

Etat: VIGUEUR

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ , Président, M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et Monsieur Maurice RONAI, membres ;

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 des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2011-334 du 29 mars 2011, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ;

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 ;

Vu la décision n°2017-265C du 27 novembre 2017 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous traitements accessibles depuis le domaine alliancefr.org :

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 24 mai 2018 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, notifié à l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE le 5 juin 2018 ;

Vu les observations écrites de l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE reçues le 6 juillet 2018, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Etaient présents, lors de la séance de la formation restreinte du 12 juillet 2018 :

- M. François PELLEGRINI, Commissaire, en son rapport ;

En qualité de représentants de l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE:

- [...] ;
- [...] ;

En qualité de conseil de l'association ALLIANCE FRANCAISE PARIS ILE DE FRANCE:

- [...] ;

Les représentants de l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE ayant pris la parole en dernier ;

A adopté la décision suivante :

1. **Faits et procédure**

L'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE (ci-après l'association) est une association créée en vertu de la loi du 1er juillet 1901, reconnue d'utilité publique, dont l'objectif est de contribuer au développement de la langue française en proposant des cours de français. Son chiffre d'affaires pour l'année 2017 est de 8 871 905 euros.

Le 26 novembre 2017, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été informée de l'existence d'un défaut de sécurité sur le sous-domaine portail.alliancefr.org faisant partie du site web

www.alliancefr.org exploité par l'association pour les besoins de son activité. Il était fait état de ce que ce défaut de sécurité permettait d'accéder à des documents contenant des données à caractère personnel à partir d'adresses URL du type https://portail.alliancefr.org/utilisateur/telecharger_document?id_document=X , où X représente un nombre entier.

Le 4 décembre 2017, en application de la décision n° 2017-265C du 27 novembre 2017 de la Présidente de la Commission, une délégation de la CNIL a procédé à des constatations en ligne sur le domaine alliancefr.org .

Au cours du contrôle, la délégation a constaté que la saisie de plusieurs adresses URL du type précité permettait de télécharger des documents contenant des données à caractère personnel tels que des factures, des certificats d'inscription à un stage ou encore des récapitulatifs des cours suivis. La délégation a ainsi été en mesure, par simple incrémentation de la valeur de X , de télécharger 15 611 documents qui contenaient tous au moins un nom et un prénom et qui pour certains, contenaient également une adresse postale et une nationalité.

Le jour même, la délégation a pris contact avec l'association par téléphone et par courriel afin de l'informer de l'existence de cette violation de données et l'a invitée à prendre les mesures nécessaires afin d'y remédier. Le 6 décembre 2017, l'association a indiqué par courriel à la délégation qu'elle allait *procéder au plus tôt à la mise en place d'un correctif empêchant cette fuite de données.* Le procès-verbal de constat n°2017-265/1 a été notifié à l'association le 14 décembre 2017.

Le 5 février 2018, la délégation de la CNIL a procédé à une mission de contrôle dans les locaux de l'association. La délégation a constaté à cette occasion que les documents qu'elle avait téléchargés au cours du contrôle en ligne du 4 décembre 2017 étaient toujours accessibles à partir des mêmes adresses URL et que 413 144 documents étaient accessibles.

L'association a expliqué que le sous-domaine portail.alliancefr.org avait été réalisé par son sous-traitant, que n'étant pas satisfaite de la dernière version livrée, elle avait décidé de dénoncer les contrats passés avec celui-ci et qu'elle avait repris l'administration et la maintenance du site en octobre 2017. L'association a expliqué qu'en raison du litige qui l'oppose à son sous-traitant, elle avait fait constater l'existence de la violation de données par un huissier de justice le 20 décembre 2017 et qu'à cette occasion, un correctif avait été mis en place. Au jour du contrôle sur place, l'association n'avait pas encore reçu le procès-verbal de constat établi par l'huissier de justice.

Par ailleurs, l'association a indiqué à la délégation qu'un courrier électronique l'informant de l'existence d'une vulnérabilité sur le sous-domaine lui avait été adressé le 20 juillet 2017 mais qu'elle n'avait pas réussi à contacter son expéditeur.

Le 23 février 2018, un second contrôle en ligne effectué par la délégation de la CNIL a fait apparaitre que les documents pouvaient toujours être téléchargés. L'association en a été informée le jour même par courrier électronique. Le procès-verbal de constat n°2017-265/3 a été notifié à l'association le 28 février 2018. Le 2 mars 2018, l'association a indiqué que des correctifs mettant fin à la violation de données avaient été mis en place.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 24 mai 2018, sur le fondement de l'article 46 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée).

A l'issue de son instruction, le rapporteur a notifié à l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE le 5 juin 2018 un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce et proposait à la formation restreinte de prononcer une sanction pécuniaire de quarante mille (40.000) euros qui serait rendue publique.

Ce rapport était accompagné d'une convocation pour la séance de la formation restreinte du 12 juillet 2018 et invitait l'association à produire des observations en réponse dans un délai d'un mois.

Le 6 juillet 2018, l'association a produit des observations écrites en réponse au rapport, réitérées oralement lors de la séance de la formation restreinte du 12 juillet suivant.

II. Motifs de la décision

Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données.

L'article 34 de la loi du 6 janvier 1978 modifiée dispose que *le responsable du 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 .*

Il appartient à la formation restreinte de décider si l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE a manqué à l'obligation de mettre en œuvre des moyens propres à assurer la sécurité des données à caractères personnel contenues dans son système d'information et en particulier, celles des utilisateurs du sous-domaine portail.alliancefr.org afin notamment que ces données ne soient pas accessibles à des tiers non autorisés.

En défense, l'association rappelle que c'est son sous-traitant qui, entre septembre 2012 et octobre 2017 était en charge de la conception du sous-domaine à l'origine de l'incident et qu'elle n'a commencé à s'approprier cet outil qu'en octobre 2017, date à laquelle elle a mis fin au contrat passé avec son sous-traitant. Elle affirme également qu'aucun utilisateur n'a exploité la vulnérabilité contenue dans les adresses URL en question et qu'en tout état de cause, son site internet ne présente aucun intérêt pour un attaquant.

Elle expose également n'avoir reçu le premier procès-verbal que le 14 décembre 2017 et avoir corrigé la vulnérabilité dès le 20 décembre 2017 à l'occasion de la réalisation du constat d'huissier. Sur ce point, elle rappelle qu'en raison du contentieux qui l'oppose à son sous-traitant, il lui était indispensable, avant toute action correctrice de sa part, de faire constater l'existence de la violation de données par un huissier de justice. Elle ajoute n'avoir été informée de la persistance de la violation que lors du contrôle sur place du 5 février 2018, puis lors de la réception du procès-verbal du contrôle en ligne du 23 février suivant.

En premier lieu, la formation restreinte relève que l'association ne conteste pas l'existence d'un incident de sécurité sur le sous-domaine portail.alliancefr.org qui a rendu accessibles 413 144 documents contenant les données à caractère

personnel des personnes suivant les cours de français qu'elle dispense.

La formation restreinte note que l'exploitation de cette vulnérabilité ne nécessitait aucune compétence particulière dans la mesure où l'accès aux documents était possible grâce à la simple modification de la valeur de X dans l'adresse URL *https://portail.alliancefr.org/utilisateur/telecharger_document?id_document=X* .

Cette vulnérabilité très fréquente aurait pu être évitée si par exemple, l'association avait mis en œuvre un moyen d'authentification permettant de s'assurer que les personnes accédant aux documents étaient bien celles dont les données personnelles étaient contenues dans lesdits documents et éventuellement accompagné d'un dispositif permettant d'éviter la prévisibilité des URL. La formation restreinte rappelle que l'exposition de données caractère personnel sans contrôle d'accès préalable est identifiée comme faisant partie des failles de sécurité les plus répandues et pour lesquelles une surveillance particulière s'impose.

En deuxième lieu, la formation restreinte rappelle que la circonstance selon laquelle une violation de données ait pu avoir pour origine une erreur commise par un sous-traitant est sans influence sur l'obligation pesant sur le responsable de traitement d'assurer un suivi rigoureux des actions menées par ce dernier. En effet, l'alinéa 3 de l'article 35 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au moment des faits, dispose que *Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.* .

La formation restreinte souligne ensuite que l'association a expliqué au cours de la procédure de contrôle qu'elle avait conscience que le logiciel livré par son sous-traitant comportait des dysfonctionnements. Dès lors, elle aurait dû faire preuve d'une vigilance accrue, notamment lorsqu'elle a été alertée au mois de juillet 2017 par une personne extérieure de l'existence d'une vulnérabilité sur son sous-domaine. Par ailleurs, l'affirmation de l'association selon laquelle aucune personne n'aurait consulté les documents à partir des URL en question ne se fonde sur aucun élément et en tout état de cause, est erronée puisqu'une personne a bien pu accéder aux données en question en juillet 2017.

Enfin, la formation restreinte rappelle que la mise en place de mesures de sécurité est une obligation incombant au responsable de traitement qui ne dépend pas de la potentielle attractivité des données traitées ou de leur valeur sur le marché. Seuls les moyens mis en œuvre pour satisfaire à cette obligation peuvent varier en fonction d'une multitude de critères tels que le nombre de données traitées, leur nature et les catégories de personnes concernées.

Au regard de ces éléments, la formation restreinte considère que l'association n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées et considère que le manquement à l'article 34 de la loi du 6 janvier 1978 modifiée est constitué.

Sur la sanction et la publicité

Aux termes du I de l'article 45 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des constats *:*

Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.

Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes :

1° Un avertissement ;

2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;

3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.

Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable, et après une procédure contradictoire, les sanctions prévues au présent I.

Les alinéas 1er et 2ème de l'article 47 de la loi précitée, dans sa version applicable au jour des constats, précisent que :

Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission.

Le montant de la sanction ne peut excéder 3 millions d'euros .

L'association considère qu'au regard des circonstances dans lesquelles est intervenue la violation de données, ni une sanction pécuniaire de 40.000 euros, ni la publicité de cette sanction ne sont justifiées.

Elle estime que la gravité du manquement n'est pas établie dans la mesure où aucune personne concernée par la violation de données n'a introduit de réclamation auprès d'elle, que les données rendues accessibles n'étaient pas sensibles et que le nombre d'utilisateur du site internet n'est pas un élément pertinent pour évaluer la gravité du manquement.

En premier lieu, la formation restreinte rappelle que l'absence de plaintes émanant d'utilisateurs et le fait que les données accessibles ne contiennent aucune donnée pouvant être qualifiée de sensible , au sens de l'article 8 de la loi

Informatique et Libertés , sont sans influence sur la caractérisation du manquement à l'obligation incombant à un responsable de traitement d'assurer la sécurité des données qu'il traite. Elle souligne en outre que la violation de données a concerné un nombre important de documents contenant tous des données identifiants tels que le nom, le prénom et l'adresse postale.

En deuxième lieu, s'agissant de la réactivité de l'association pour mettre fin à la violation de données, la formation restreinte note que dès le 4 décembre 2017, la délégation de contrôle de la CNIL a adressé à l'association un courriel faisant état de l'existence de la violation de données et qui contenait le type d'adresse URL à l'origine de cette violation. Elle était donc, dès cette date, en mesure de commencer des investigations sur son sous-domaine. La formation restreinte souligne que contrairement à ce que soutient l'association, il n'a pas été mis fin à la violation de données le 20 décembre 2017 puisque la délégation de la CNIL a constaté sa persistance une première fois lors du contrôle sur place du 5 février 2018 puis une seconde fois lors du contrôle en ligne du 23 février 2018. Ce n'est que le 2 mars 2018 que l'association a informé la CNIL qu'il avait été mis définitivement fin à la violation de données.

En troisième lieu, la formation restreinte estime que la gravité du manquement est caractérisée, notamment au regard du caractère élémentaire de l'incident de sécurité constitué par l'absence de mesures d'authentification des personnes accédant aux documents et par le caractère prévisible des adresses URL permettant de les télécharger.

Au regard des éléments développés ci-dessus, les faits constatés et le manquement constitué à l'article 34 de la loi du 6 janvier 1978 modifiée justifient que soit prononcée une sanction d'un montant de 30.000 (trente mille) euros.

Enfin, la formation restreinte considère qu'au regard de la gravité du manquement précité, du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les responsables de traitement et les internautes quant aux risques pesant sur la sécurité des données, il y a lieu de rendre publique sa décision.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide :

- **de prononcer à l'encontre de l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE une sanction pécuniaire d'un montant de trente mille (30.000) euros ;**
- **de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.**

Le Président

Jean-François CARREZ

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'Etat dans un délai de deux mois à compter de sa notification.

Nature de la délibération: SANCTION
Date de la publication sur legifrance: 27 septembre 2018