Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN 2017-002 du 13 avril 2017

Délibération de la formation restreinte n° SAN 2017-002 du 13 avril 2017 prononçant une sanction pécuniaire à l'encontre de la société ALLOCAB

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, M. Philippe GOSSELIN, M. Maurice RONAI, Mme Dominique CASTERA et Mme MITJAVILLE, 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 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

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 ;

Vu la décision n° 2015-076C en date du 19 février 2015 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 mis en œuvre dans le cadre de la gestion et de l'exploitation du site internet ALLOCAB.COM et des applications correspondantes ;

Vu la décision n° 2015-062 du 10 novembre 2015 de la Présidente de la Commission nationale de l'Informatique et des libertés mettant en demeure la société ALLOCAB ;

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 3 janvier 2017 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, du 12 janvier 2017 ;

Vu les observations écrites versées par la société ALLOCAB le 13 février 2017 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 23 février 2017 :

Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société ALLOCAB: […] ;

En qualité de conseil de la société ALLOCAB : […].

Madame Nacima BELKACEM, commissaire du Gouvernement, n'ayant pas formulé d'observation ;

Les représentants de la société ALLOCAB ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

Faits et procédure

La société ALLOCAB (ci-après la société) est une société spécialisée dans le transport de particuliers. Fondée en 2011, elle emploie environ […] personnes et a réalisé un chiffre d'affaires […].

Le 16 janvier 2015, une plainte a été adressée à la CNIL par un client de la société s'agissant de la conservation de ses coordonnées bancaires au moment du paiement de ses réservations en ligne. Postérieurement, une mission de contrôle sur place a été diligentée au sein des locaux de la société ALLOCAB en application de la décision n° 2015-076C du 19

février 2015 de la Présidente de la CNIL. À cette occasion, des manquements à la loi n° 78-17 du 6 janvier 1978 modifiée (ci-après la loi Informatique et Libertés) ont été constatés et le procès-verbal n° 2015-076 du 5 mars 2015 a été notifié à la société.

Par décision n° 2015-062 du 10 novembre 2015 de la Présidente de la CNIL, la société a fait l'objet d'une procédure de mise en demeure lui enjoignant, dans le délai de trois mois, d'adopter les mesures correctives suivantes :

- […] ;

- définir une durée de conservation des données présentes en base, en fonction des finalités pour lesquelles ces données sont collectées et traitées ; en particulier, veiller à ce que les données relatives au cryptogramme ne soient pas conservées au-delà du temps nécessaire à la réalisation de la transaction et procéder à la purge des données des clients ayant demandé la suppression de leurs comptes ;

- […] ;

- prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données à caractère personnel des utilisateurs, et notamment :

[…] ;

modifier la procédure de confirmation du mot de passe des utilisateurs afin que celui-ci ne soit plus communiqué en clair, par exemple, en leur proposant, d'une part, de recevoir par courrier électronique soit un mot de passe aléatoire, utilisable une seule fois afin de leur permettre de redéfinir leur mot de passe, soit un lien vers une page leur permettant d'enregistrer un nouveau mot de passe et en procédant, d'autre part, au stockage haché des mots de passe en base de données à l'aide, par exemple, de l'algorithme SHA 256 avec utilisation d'un sel qui devra faire l'objet d'un stockage sur un espace distinct de celui dans lequel sont stockés les mots de passe (en dehors de la base de données) ;

modifier la procédure de récupération du mot de passe des utilisateurs afin que celui-ci ne soit plus communiqué en clair ;

imposer, pour chaque mot de passe, une robustesse suffisante.

En l'absence de réponse dans le délai imparti, un courrier de relance a été adressé à la société le 31 mars 2016.

Par courrier en date du 28 avril 2016, la société a communiqué des premiers éléments en réponse à la mise en demeure qui lui a été adressée.

La Présidente de la CNIL ayant relevé que la conformité n'était pas pleinement acquise pour quatre des manquements constatés à savoir […], l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement et l'obligation d'assurer la sécurité et la confidentialité des données, une demande de compléments a été adressée à la société le 12 juillet 2016.

La société n'ayant pas répondu à cette demande de compléments, un courrier de relance lui a été adressé le 9 septembre 2016.

Par courrier en date du 14 septembre 2016, la société a indiqué avoir entrepris diverses actions complémentaires afin de se conformer aux termes de la mise en demeure qui lui a été adressée. La société a ainsi précisé avoir modifié […], pris des mesures afin de modifier le processus de paiement pour ne plus conserver les cryptogrammes des cartes bancaires, mis en place une politique de durée de conservation des données des utilisateurs et prévu une mise à jour du service d'authentification afin d'uniformiser la politique des mots de passe.

La société a précisé que les évolutions relatives au processus de paiement (suppression des cryptogrammes stockés en base) ainsi qu'à l'uniformisation de la politique des mots de passe étaient prévues pour la fin du mois de septembre 2016. Elle a également indiqué qu'aucun mot de passe n'était stocké en clair dans sa base de données. S'agissant de la durée de conservation des données relatives à ses utilisateurs, la société a précisé que les modifications envisagées devraient être finalisées pour le 1er octobre 2016.

En application de la décision n° 2015-076C du 19 février 2015 précitée, un contrôle sur place a été diligenté au sein des locaux de la société ALLOCAB le 12 décembre 2016 afin de vérifier les mesures prises par cette dernière. Des éléments complémentaires ont été demandés à la société sous huit jours, laquelle a répondu par courrier en date du 22 décembre 2016.

Il résulte de ce contrôle que plusieurs des mesures annoncées par la société dans son courrier du 14 septembre 2016 n'ont pas été mises en place. Au regard des manquements persistants au-delà du délai imparti par la mise en demeure, la Présidente de la CNIL a désigné
M. François PELLEGRINI en qualité de rapporteur, le 3 janvier 2017, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée.

À l'issue de son instruction, le rapporteur a fait notifier à la société, par porteur, le 13 janvier 2017, un rapport détaillant les manquements à la loi Informatique et Libertés qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la CNIL de prononcer une sanction pécuniaire de 50.000 euros, rendue publique.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 23 février 2017 indiquant à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites.

Le 13 février 2017, la société a produit des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 23 février 2017.

Motifs de la décision

A.Un manquement à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement

L'article 6-5° de la loi du 6 janvier 1978 modifiée dispose que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées .

La société a été mise en demeure de définir une durée de conservation des données présentes en base, en fonction des finalités pour lesquelles ces données sont collectées et traitées et, en particulier, veiller à ce que les données relatives au cryptogramme ne soient pas conservées au-delà du temps nécessaire à la réalisation de la transaction. Il a également été enjoint à la société de procéder à la purge des données des clients ayant demandé la suppression de leurs comptes.

Il appartient à la formation restreinte de décider si la société s'est conformée aux termes de la mise en demeure ou a manqué à l'obligation lui incombant de définir et de respecter une durée de conservation proportionnée à la finalité du traitement.

En défense, si la société ne conteste pas les faits qui lui sont reprochés, elle fait principalement valoir qu'elle a porté une attention particulière aux demandes formulées par la CNIL et qu'elle s'est montré diligente tout au long de la procédure en se mettant en conformité avec un grand nombre des manquements qui étaient relevés. La société précise, en tout état de cause, que sa difficulté à se conformer aux injonctions formulées à son encontre, dans le délai initialement imparti, était due aux faibles moyens financiers et humains dont elle disposait.

En premier lieu, s'agissant de la purge automatique des données relatives à des comptes inactifs depuis quinze mois ou plus, elle précise ainsi avoir, dès l'été 2016, engagé des travaux de mise en conformité et avoir rencontré de nombreux problèmes techniques. La société indique que des correctifs ont été mis en œuvre, dont la finalisation est intervenue la dernière semaine de novembre 2016.

Elle relève également que si, au jour du second contrôle, la délégation a effectivement constaté que des données relatives à des comptes inactifs étaient encore présentes dans son système d'information, seuls dix comptes d'utilisateurs étaient concernés sur l'ensemble des clients de la société ALLOCAB.

La société précise en outre avoir mené un travail d'investigation pour comprendre les raisons de ce dysfonctionnement et avoir travaillé durant tout le mois de décembre 2016 à la réécriture de la procédure de purge, celle-ci étant pleinement effective depuis la fin du mois de janvier [2017] .

En second lieu, en ce qui concerne la suppression des cryptogrammes visuels, la société a indiqué que cette conservation se justifiait initialement par les exigences techniques imposées par son prestataire de paiement. Elle précise avoir pris la décision de changer de prestataire de paiement, ce changement n'ayant pu intervenir qu'au mois d'octobre 2016 avant qu'un problème majeur ne l'oblige à revenir à son ancien prestataire.

La société indique que la modification de l'interface de paiement a ainsi été opérée à la fin du mois de janvier 2017 et qu'il n'y a plus, au jour de l'audience, aucun cryptogramme visuel stocké en base. Elle produit à cet égard un constat d'huissier.

La formation restreinte relève tout d'abord que malgré l'échéance du délai imparti par la mise en demeure, plusieurs échanges ont eu lieu avec la société afin de l'accompagner dans une démarche de mise en conformité. À cet égard, le second contrôle est intervenu près de deux mois après le courrier en réponse de la société du 14 septembre 2016 annonçant l'effectivité des mesures de conformité entreprises.

La formation restreinte considère également qu'il n'y a pas lieu de minimiser le nombre de comptes non purgés ou de cryptogrammes conservés à la date du 12 décembre 2016 dès lors que le délai de mise en conformité était largement expiré et qu'aucun cryptogramme n'aurait dû être stocké par la société à cette date.

En tout état de cause, la formation restreinte relève qu'aucun élément permettant effectivement d'attester des dysfonctionnements dont se prévaut la société n'a été porté à sa connaissance dans le cadre de la présente procédure ni à celle des services de la CNIL tout au long de l'instruction.

Le manquement aux obligations découlant de l'article 6-5° de la loi du 6 janvier 1978 modifiée est, dès lors, caractérisé.

B.Un 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 la société ALLOCAB a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel contenues dans son système d'information.

En défense, si la société n'entend pas contester les constatations effectuées par les services de la CNIL, elle fait en premier lieu valoir que l'article 34 de la loi du 6 janvier 1978 modifiée n'apporte aucune précision quant à la robustesse susceptible d'être imposée pour la création et l'utilisation des mots de passe des utilisateurs, considérant ainsi que le grief relatif à l'obligation d'assurer la sécurité et la confidentialité des données lui est inopposable.

Elle considère également qu'au regard des exigences qui lui étaient imposées, la Présidente a manifestement anticipé sur le fruit des travaux menés par la CNIL dans le cadre de la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

La société précise enfin qu'en tout état de cause, avant même le premier contrôle de la CNIL, les mots de passe devaient comprendre huit caractères. Comme annoncé dans son courrier du 28 avril 2016, elle indique avoir travaillé à la mise en œuvre d'une politique de gestion des mots de passe, laquelle a fait l'objet d'un dysfonctionnement technique révélé lors du second contrôle de la CNIL.

En deuxième lieu, s'agissant de la transmission en clair de l'identifiant et du mot de passe dans le courrier électronique de confirmation de création de compte, la société indique avoir remédié au dysfonctionnement constaté. Elle produit à cet égard un constat d'huissier.

En troisième lieu, en ce qui concerne la méthode de stockage du sel, la société précise que le sel stocké sur l'objet utilisateur avec le mot de passe encrypté est unique pour chaque utilisateur et changé à chaque fois qu'il modifie son mot de passe . Elle estime ainsi que cette modalité de stockage du sel dans un fichier distinct de celui où figure le mot de passe hashé et encrypté ne semble pas faire peser un quelconque risque pour la sécurité des données des utilisateurs .

La formation restreinte rappelle tout d'abord que le dispositif de la mise en demeure adressée à la société était sans ambiguïté et que cette dernière ne saurait désormais arguer du caractère imprécis de l'article 34 de la loi du 6 janvier 1978 modifiée. Elle relève à cet égard que dans le cadre des courriers adressés à la CNIL les 28 avril et 14 septembre 2016, la société a indiqué être en train d'opérer une modification invitant ses clients à choisir un mot de passe composé d'au moins huit caractères avec trois critères de complexité et accompagné d'un dispositif leur indiquant le degré de force et de sécurité du mot de passe choisi.

Elle rappelle également qu'en l'espèce, il ne s'agissait pas d'imposer de manière anticipée à la société les dispositions de la recommandation du 19 janvier 2017 précitée mais bien celles de l'article 34 de la loi du 6 janvier 1978 modifiée. En tout état de cause, la formation restreinte relève que s'il avait été fait application de ladite recommandation, ce n'est pas huit mais douze caractères qui auraient été demandés dans le cadre de la composition des mots de passe.

Elle relève par ailleurs qu'il n'est pas contesté qu'à la date du 12 décembre 2016, des mots de passe composés d'un seul caractère étaient acceptés par le système d'information de la société. De la même manière, la formation restreinte observe que, contrairement aux réponses fournies par la société dans son courrier du 28 avril 2016, l'identifiant et le mot de passe des utilisateurs étaient toujours transmis en clair à l'utilisateur à la date du second contrôle.

La formation rappelle enfin que le stockage du sel dans un espace distinct de celui où sont stockés les mots de passe (et non dans un même fichier) constitue une précaution élémentaire de nature à assurer la sécurité et la confidentialité des données.

Sur la base de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 34 de la loi du 6 janvier 1978 modifié est constitué.

Sur la sanction et la publicité

La formation restreinte considère que les manquements aux articles 6-5° et 34 de la loi du 6 janvier 1978 modifiée ont persisté bien au-delà de l'échéance du délai imparti par la mise en demeure de la Présidente de la Commission.

Prenant en considération le fait, établi par constat d'huissier, que la société s'était mise en conformité au 13 février 2017, la formation restreinte estime justifié le prononcé, à son encontre, d'une sanction d'un montant de 15 000 euros.

Compte tenu de la persistance dans le temps de plusieurs manquements formulés à l'encontre de la société, malgré les nombreuses diligences effectuées à son égard par les services de la CNIL, la formation restreinte décide de rendre publique sa décision. Elle estime nécessaire de sensibiliser les personnes et les responsables de traitement aux droits et obligations issus de la loi Informatique et Libertés , en particulier, à l'importance de répondre aux demandes de la Présidente et de mettre effectivement en œuvre les mesures annoncées.

PAR CES MOTIFS

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

de prononcer à l'encontre de la société ALLOCAB une sanction pécuniaire d'un montant de 15.000 € ;

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 peut 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: 25 avril 2017