Le : 10/05/2019

Date de publication sur legifrance: 28/06/2018

Commission Nationale de l'Informatique et des Libertés

Délibération n°2018-003 du 21 juin 2018
Délibération de la formation restreinte n° SAN-2018-003 du 21 juin 2018 prononçant une sanction pécuniaire à l'encontre de l'Association pour le Développement des Foyers

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, de M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et M. 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 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 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° 2017-147C du 12 juin 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 de données à caractère personnel accessibles à partir du domaine adef-logement.fr ;
Vu la décision n° 2017-157C de la Présidente de la CNIL du 12 juin 2017 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de l'association ADEF Hébergement ;
Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur devant la formation restreinte, en date du 24 janvier 2018 ;
Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié par porteur à l'association ADEF le 23 février 2018 ;
Vu les observations écrites de l'association ADEF reçues le 16 avril 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 3 mai 2018 :

- Monsieur François PELLEGRINI, Commissaire, en son rapport ;
- En qualité de représentant de l'association ADEF :
- En qualité de conseil de l'association ADEF :
- X ;
- Y ;

M. Michel TEIXEIRA, Commissaire du Gouvernement adjoint, n'ayant pas formulé d'observations ;

Les représentants de l'association ADEF ayant pris la parole en dernier ;
A adopté la décision suivante :

- <u>Faits et procédure</u>

L'Association pour le Développement des Foyers (ci-après ADEF ou l'association) est une association de droit privé à but non lucratif créée en vertu de la loi du 1er juillet 1901. Elle a pour mission la mise à disposition de logements dans des résidences et foyers pour personnes en difficulté sociale, notamment des étudiants, des familles monoparentales et des travailleurs migrants.
L'association emploie environ 270 salariés et a réalisé en 2016 un chiffre d'affaires de 37,6 millions d'euros. Son siège est situé au 19, rue Baudin à Ivry-sur-Seine (94200).
Le 11 juin 2017, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a été alertée de l'existence d'un défaut de sécurité permettant d'accéder à des avis d'imposition de bénéficiaires de l'association, à partir d'une recherche effectuée sur le moteur de recherche Google.
En application de la décision n° 2017-147C de la Présidente de la Commission du 12 juin 2017, une délégation de la CNIL a procédé à une mission de contrôle en ligne le 15 juin suivant sur les traitements mis en œuvre par l'association. Le procès-verbal de constat n°2017-147/1 dressé à l'issue de cette mission, a été adressé à l'association par courrier électronique (courriel) et par courrier le 20 juin 2017.
Au cours du contrôle, la délégation a effectué une demande de logement en renseignant le formulaire présent sur le site web de l'association http://www.adef-logement.fr/ et a constaté qu'une modification du chemin de l'URL affichée dans le navigateur permettait d'accéder aux documents enregistrés par d'autres demandeurs.
En outre, la délégation a effectué la recherche suivante directement au sein du moteur de recherche Google *site:adef-logement.fr filetype:pdf impot .* Elle a constaté que des avis d'imposition sur les revenus figuraient dans la liste de résultats affichée.
Le 15 juin 2017, la délégation a pris contact avec l'association par téléphone et par courriel pour l'informer de l'existence de cette violation de données à caractère personnel et lui demander de prendre les mesures correctives nécessaires afin d'y remédier. Par courriel du 19 juin suivant, la Commission a informé l'association que les données à caractère personnel étaient toujours librement accessibles sur le domaine adef-logement.fr .
Le 20 juin 2017, l'association a informé la CNIL qu'elle avait saisi son service informatique afin qu'il contacte l'hébergeur du site internet et a précisé que la Commission serait informée au plus vite des mesures correctrices prises.
En application de la décision n° 2017-157C du 12 juin 2017 de la Présidente de la CNIL, une délégation de la Commission a procédé à une mission de contrôle dans les locaux de l'association le 21 juin 2017, notamment afin de vérifier les mesures correctrices prises à la suite de la révélation de la violation de données. Le procès-verbal de contrôle n° 2017-157/1 a été notifié à l'association le 23 juin 2017.
Lors du contrôle sur place, l'association a informé la délégation qu'elle avait contacté la société […], qui avait développé le site web en 2012, afin qu'elle mette en place les mesures correctives. Il a cependant été constaté à cette occasion que les données des personnes étaient toujours accessibles sur Internet par une simple modification de l'URL.
Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 24 janvier 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).
À l'issue de son instruction, le rapporteur a notifié à l'association ADEF, par porteur, le 23 février 2018, un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer une sanction pécuniaire qui ne saurait être inférieure à cent cinquante mille (150.000) euros et qui serait rendue publique.
Était également jointe au rapport une convocation à la séance de la formation restreinte du

5 avril 2018 indiquant à l'association qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites.

Par courrier du 13 mars 2018, l'association a sollicité de la part du Président de la formation restreinte le report de la séance. Cette demande a été acceptée le 21 mars 2018 et la séance a été reportée au 3 mai suivant.

Le conseil de l'association a en outre sollicité, par courrier du 14 mars 2018, la communication des actes de nomination et d'habilitation des deux agents contrôleurs de la CNIL à procéder à des contrôles, ainsi que de la mise en demeure adressée par la Présidente de la CNIL à l'association conformément au I de l'article 45 de la loi du 6 janvier 1978 modifiée.

Par courrier du 20 mars 2018, le secrétaire général de la CNIL a indiqué à l'association que les deux agents de la CNIL avaient été habilités à procéder à des missions de vérification par délibération n° 2017-150 du 9 mai 2017 disponible sur le site web www.legifrance.gouv.fr et a fourni les deux ordres de mission sollicités. En outre, il a informé le conseil de l'association qu'aucune mise en demeure n'avait été adoptée par la Présidente à l'encontre de l'association préalablement à l'envoi du rapport de sanction.

De plus, le conseil de l'association a demandé, par courrier du même jour, à la Commission la communication des annexes et pièces jointes des procès-verbaux des contrôles ainsi que la justification que les contrôleurs avaient opéré, préalablement au contrôle en ligne, toute mesure garantissant la réalité des faits constatés et conférant force probante aux constats.

Par courrier du 6 avril 2018, le secrétaire général de la CNIL a répondu que le procès-verbal de constatation et les pièces issues du contrôle avaient été gravés sur DVD-Rom et adressés à l'association le 20 juin 2017. L'association et son conseil ont également été informés qu'ils pouvaient obtenir communication sur place des pièces du dossier.

Le 16 avril 2018, l'association a produit des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 3 mai suivant.

· Motifs de la décision

1. Sur les motifs de nullité de la procédure soulevés par l'association

En premier lieu, l'association soutient que la procédure de sanction est entachée de nullité dès lors qu'elle méconnaît le I de l'article 45 de la loi du 6 janvier 1978 modifiée par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

Le I de l'article 45 de la loi du 6 janvier 1978 modifiée prévoit que :

I. - 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.
L'association fait valoir qu'en application de cette disposition, elle aurait dû recevoir une mise en demeure préalable de la Présidente avant l'envoi du rapport de sanction et qu'en l'absence d'une telle décision, la procédure de sanction initiée devant la formation restreinte est nulle.
La formation restreinte relève qu'il résulte de la lettre même de l'article 45 de la loi du 6 janvier 1978 précité que le prononcé d'une sanction n'est pas subordonné à l'adoption préalable systématique d'une mise en demeure. À cet égard, elle souligne que le dernier alinéa de cet article prévoit expressément que *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 prévue au présent I* .
Elle rappelle également que l'objet de la réforme introduite par la loi pour une République numérique était d'élargir la gamme des sanctions directes qu'elle peut appliquer, en autorisant le prononcé d'une sanction pécuniaire sans mise en demeure préalable, alors qu'auparavant, la formation restreinte ne pouvait en pareil cas prononcer qu'un avertissement.
La loi précise expressément que lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure (qui ne peut par construction avoir d'effet que pour l'avenir et non pour le passé), la formation restreinte peut prononcer les sanctions prévues.
L'interprétation de l'article 45 de la loi du 6 janvier 1978 modifiée suggérée par la défense aurait pour effet de rendre impossible la sanction des infractions passées. Elle constituerait même une raison, pour un responsable de traitement ayant causé ou subi une violation de données, de s'abstenir de prendre aucune mesure corrective et d'attendre que lui soit éventuellement adressée une mise en demeure, le seul fait de s'y conformer faisant alors obstacle au prononcé d'une sanction.
La formation restreinte considère qu'en l'espèce, les effets du manquement constaté ne pouvaient être corrigés par le biais d'une mise en demeure (à savoir la libre accessibilité des données à caractère personnel pendant la durée de l'incident de sécurité) mais que le manquement pouvait être directement sanctionné, en vertu du dernier alinéa du I de l'article 45 de la loi du 6 janvier 1978 modifiée.
En second lieu, l'association soutient qu'elle a reçu le procès-verbal de constatation en ligne du 15 juin 2017, le 22 juin suivant, soit après le contrôle sur place de la délégation de la CNIL. Elle soutient que ce n'est qu'à ce stade qu'elle a pu prendre connaissance de la procédure en cours, sans mesurer les sanctions encourues et pouvoir réellement exercer ses droits de la défense dans le cadre d'une procédure contradictoire.
La formation restreinte relève cependant qu'il ressort des pièces jointes au rapport que le procès-verbal du contrôle en ligne a été envoyé à l'association par courriel le 20 juin 2017 ainsi que par courrier le même jour. Si elle a effectivement reçu le procès-verbal sous format papier le 22 juin 2017, l'association avait connaissance au jour du contrôle sur place, du 21 juin 2017, des constatations effectuées par la Commission au cours du contrôle en ligne.

La formation restreinte estime donc que l'association a eu connaissance dès le 20 juin 2017, de la nature, du jour, de l'heure ainsi que l'objet du contrôle effectué par la délégation de la CNIL le 15 juin 2017. À cet égard, la formation restreinte relève qu'il ressort du procès-verbal établi lors du contrôle sur place que l'association indique avoir reçu le procès-verbal du contrôle en ligne le 20 juin 2017.
La formation restreinte considère en outre que les droits de la défense n'ont pas été méconnus dès lors que l'association a été informée de son droit de se faire assister ou représenter par le conseil de son choix, lors du contrôle sur place du 21 juin 2017, et dès lors qu'elle a formulé, par le biais de son représentant, des observations écrites et orales en réponse au rapport effectué à son encontre.
Enfin, la formation restreinte relève qu'aucun autre motif de nullité ne résulte de l'instruction devant elle.

Par conséquent, les moyens tirés de la nullité de la procédure de sanction ne peuvent qu'être écartés.

- **Sur le manquement à l'obligation d'assurer la sécurité des données au titre de l'article 34 de la loi du 6 janvier 1978 modifiée**

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 ADEF 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 et, en particulier, celles des utilisateurs du site web http://www.adef-logement.fr afin notamment que ces données ne soient pas accessibles à des tiers non autorisés.
En défense, l'association reconnaît l'existence de l'incident de sécurité constaté.
La formation restreinte note qu'il est avéré que les services de la CNIL ont pu accéder aux documents enregistrés par les utilisateurs du site web http://www.adef-logement.fr .
En premier lieu, tout en soulignant la diligence de l'association qui a réagi rapidement après la révélation de l'incident pour le corriger, la formation restreinte relève que les mesures élémentaires de sécurité n'avaient pas été prises en amont du développement de son site internet.
En effet, la formation restreinte note que la modification d'un mot présent dans l'URL du formulaire d'une demande de logement tel que passeport ou cni permettait à des tiers non autorisés d'accéder aux documents fournis par les utilisateurs de son site web. Cette violation de données a été rendue possible par l'absence de mise en place, par l'association, d'un dispositif permettant d'éviter la prévisibilité des URL.
En outre, la formation restreinte considère que l'association aurait dû *a minima* mettre en place une fonction modifiant la dénomination des fichiers enregistrés par les personnes, lors du téléversement de ceux-ci sur son répertoire de stockage, afin d'éviter qu'une personne n'identifie le chemin d'accès aux dossiers enregistrés.
La formation restreinte estime que l'association aurait dû mettre en place de telles mesures élémentaires qui, au surplus, ne requéraient pas de développements importants, ni coûteux.
De plus, la formation restreinte relève que les personnes pouvaient effectuer des demandes de logement en ligne sans qu'aucune procédure d'identification ou d'authentification des utilisateurs du site web n'ait été mise en place pour protéger les informations enregistrées. La formation restreinte estime que l'association aurait dû mettre en place une restriction d'accès aux documents mis à la disposition des clients *via* un espace réservé à chaque personne, accessible grâce à un identifiant et un mot de passe.

L'association aurait dû, en outre, si elle ne souhaitait pas créer de comptes dédiés à chaque utilisateur, mettre en œuvre un moyen permettant de s'assurer que les personnes accédant aux documents enregistrés étaient bien à l'origine de la demande (par exemple grâce à un cookie identifiant de session). Elle considère ainsi que la mise en place de telles fonctionnalités constitue une précaution d'usage essentielle dont la mise en œuvre aurait permis de réduire significativement le risque de survenance de la violation de données constatée.
Par ailleurs, la formation restreinte relève que l'association n'avait pas non plus pris de mesures visant à protéger les répertoires contenant les documents des demandeurs de logement, directement accessibles depuis Internet. À cet égard, la formation restreinte relève que ce n'est qu'après l'intervention de la Commission auprès de l'association que des mesures ont été prises visant à protéger les documents concernés par l'incident et les rendre inaccessibles à des tiers non autorisés en les déplaçant *dans un dossier privé .*
En deuxième lieu, la formation restreinte relève que l'exploitation de la violation de données ne nécessitait aucune compétence technique particulière. Elle rappelle en effet que pour accéder aux documents d'autres clients, il suffisait de modifier le chemin des URL des formulaires de demande qui contenaient le nom du document enregistré par la personne. Ainsi, il était particulièrement aisé pour une personne d'inscrire dans une URL le nom d'un document qu'elle souhaitait voir afficher, tel qu'un bulletin de salaire ou une carte d'identité. La formation restreinte rappelle également que les données étaient librement accessibles en effectuant une recherche au sein du moteur de recherche Google, augmentant ainsi le risque que l'incident soit exploité par des tiers non autorisés.
La formation restreinte rappelle en outre que, de manière générale, l'exposition de données à caractère personnel sans contrôle d'accès préalable, est identifiée comme faisant partie des failles de sécurité pour lesquelles une surveillance particulière s'impose et doit, en conséquence, faire l'objet de vérifications notamment dans le cadre d'audits de sécurité. À cet égard, la formation restreinte souligne l'importance de procéder à un protocole complet de test en amont de la mise en production d'un site internet. Il apparaît également que l'association n'a pas procédé, après le déploiement des sites internet, aux vérifications régulières qui lui incombaient quant aux mesures de sécurité mises en place.
La formation restreinte estime, par conséquent, que l'association n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées.
En troisième lieu, l'association précise que l'incident n'a pas concerné tous les dossiers de demandes de logement effectuées en ligne, mais uniquement les documents fournis par des personnes n'ayant pas finalisé leur démarche sur le site internet. Elle explique que c'est la raison pour laquelle l'accès à certaines pièces n'était pas sécurisé.
La formation restreinte considère qu'une telle explication, outre qu'elle démontre une conservation de données à caractère personnel pendant un durée non justifiée, est sans incidence sur la caractérisation du manquement dès lors que l'association était tenue de s'assurer de la sécurité de toutes les données à caractère personnel traitées, même celles concernant des personnes ne validant pas leur demande de logement.
Sur la base de ces éléments, elle considère que le manquement à l'article 34 de la loi du 6 janvier 1978 modifiée est constitué.
III. Sur la sanction et la publicité
Aux termes des alinéas 1er et 2ème de l'article 47 de la loi du 6 janvier 1978 modifiée, *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 soutient que la sanction qui serait prononcée à son encontre ne devrait être que symbolique. Elle soutient qu'une sanction d'un montant de 150.000 euros proposée par le rapporteur serait disproportionnée au regard des critères posés par l'article 47 de la loi du 6 janvier 1978 modifiée dès lors qu'elle indique avoir coopéré avec la délégation de contrôle de la CNIL et avoir mis en place des mesures rapides afin de corriger l'incident.
En premier lieu, la formation restreinte considère que la gravité de la violation est caractérisée en raison de la nature des données concernées.
En effet, la violation a rendu accessibles des documents officiels, dans leur intégralité, tels que des justificatifs d'identité (passeports, titres de séjour et cartes d'identité), des bulletins de salaire, des avis d'imposition ou encore des attestations de paiement de la Caisse d'allocations familiales. En outre, ces documents contiennent une multitude de données d'identification des utilisateurs du site web telles que des noms, prénoms, dates de naissance, coordonnées postales, numéro d'inscription au répertoire national d'identification des personnes physiques ou IBAN.
Il apparaît, en outre, que certaines informations accessibles relèvent de la vie privée dès lors que les documents permettent de connaître le salaire des personnes, leur revenu fiscal de référence, leur statut marital ou leur nombre d'enfants et de savoir si elles perçoivent l'aide personnalisée au logement.
La formation restreinte estime qu'il appartenait à l'association, compte tenu de la quantité et de la nature des données traitées, d'être particulièrement vigilante sur la sécurité de celles-ci.
En second lieu, la formation restreinte considère que la gravité du manquement est également caractérisée en raison du nombre de documents et de personnes concernées par la violation.
La formation restreinte relève qu'il ressort des pièces du dossier qu'à la date de l'incident de sécurité, 42 652 documents étaient stockés sur le disque dur de l'association avec les formulaires de demande remplis par les utilisateurs. La délégation de contrôle a pu télécharger un échantillon de 385 documents, après dédoublonnage, hébergés dans les répertoires de l'association. Il est établi que le défaut de sécurité a permis à la délégation de contrôle d'accéder aux documents stockés dans ces répertoires. Il apparaît donc que l'incident a rendu accessibles un grand nombre de documents et a concerné un nombre important de personnes.
La formation restreinte note, toutefois, que l'association a réagi rapidement après avoir eu connaissance de la violation de données en mettant en place des mesures correctrices dans un délai raisonnable après avoir été alertée par la CNIL. Elle prend également acte de ce que l'association a coopéré avec la Commission dans le cadre des échanges entretenus avec ses services à la suite des contrôles en ligne ainsi que lors du contrôle sur place.
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 pécuniaire d'un montant de soixante quinze mille (75.000) euros.
Enfin, la formation restreinte considère qu'au regard des éléments précités sur la nature des données en cause, 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 pour le Développement des Foyers une sanction pécuniaire d'un montant de 75.000 (soixante quinze mille) euros ;**
- **rendre publique sa décision, 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.