Date de publication sur legifrance: 30/10/2018

**Commission Nationale de l'Informatique et des Libertés**

**Décision n°MED-2018-041 du 8 octobre 2018**
**Décision n° MED 2018-041 du 8 octobre 2018 mettant en demeure l'association « 42 »**

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe 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, abrogée par le règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu le Code pénal ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 45 ;

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° 2018-030C du 2 février 2018 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 auprès de l'association 42 .

Vu les procès-verbaux de contrôle n° 2018-030/1 du 12 février 2018 et 2018-030/2 du 13 février 2018;

Vu les autres pièces du dossier ;

I - Les faits constatés

L'association 42 (ci-après l'association ), sise 96 boulevard de Bessières à Paris (75017), est une association à but non lucratif qui a créée l'école 42 en 2013 (ci-après l'école ). L'école, qui emploie 33 salariés, a vocation à former des étudiants dans le domaine de l'informatique. Environ 800 étudiants y sont inscrits chaque année. […]. Aucun cours n'est dispensé par des enseignants, les étudiants créent des projets puis se corrigent entre eux. Des intervenants extérieurs sont ponctuellement amenés à intervenir auprès des étudiants.

En application de la décision n° 2018-030C du 2 février 2018 de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission ), une délégation de la CNIL a procédé à une mission de contrôle sur place auprès de l'association les 12 et 13 février 2018. La mission a notamment eu pour objet de vérifier la conformité à la loi 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 ) de l'ensemble des traitements de données à caractère personnel mis en œuvre par l'association.

En ce qui concerne le dispositif de vidéosurveillance au sein de l'établissement
L'association a indiqué qu'elle avait mis en place un système de vidéosurveillance comportant 60 caméras à des fins de protection des biens et des personnes. La délégation a constaté que parmi les caméras installées, certaines permettent de visualiser les espaces de travail où sont installés les postes informatiques à disposition des étudiants, l'intérieur d'un amphithéâtre, des espaces de pause, une entrée desservant les sanitaires, ainsi que les postes de travail de plusieurs membres du personnel administratif.
L'association a indiqué que le personnel administratif et les agents de sécurité ont accès à l'ensemble des images issues du dispositif et que les étudiants ont seulement accès en temps réel aux images issues des caméras visualisant les lieux qui leur sont accessibles.
Il a été précisé à la délégation que le personnel et les étudiants sont informés du dispositif par le biais d'une mention dans le règlement intérieur et que les personnes extérieures sont informées grâce à des autocollants apposés sur les portes d'entrée de l'école. La délégation a enfin été informée que les postes de travail des agents de sécurité qui ont accès au dispositif de vidéosurveillance est protégé par un mot de passe composé de 5 caractère alphanumériques.
En ce qui concerne la gestion administrative des étudiants
L'association a indiqué que pour intégrer l'école, chaque élève doit réussir des tests d'admissibilité qui se déroulent en deux phases. Les candidats doivent tout d'abord se créer un compte sur le site de l'école puis passer un premier test sur internet. Ceux qui réussissent sont ensuite invités à passer une série de tests au sein de l'école. […]. La délégation a constaté qu'aucune information relative au traitement des données n'est délivrée aux candidats, ni au moment de leur inscription aux différents tests, ni à l'occasion de leur entrée dans l'école.
Il a été indiqué à la délégation que les comptes crées par les étudiants ne sont jamais supprimés, quel que soit les résultats obtenus aux tests […]. L'école a expliqué qu'une personne ayant réussi les tests d'admission peut s'inscrire lorsqu'elle le souhaite et non pas nécessairement à la prochaine rentrée scolaire. La délégation a été informée de ce que les données des étudiants relatives à leur suivi administratif sont conservées sans limite de temps.
Par ailleurs, il a été constaté dans la partie de la base de données dédiée à la gestion des étudiants, des commentaires tels que : diagnostiqué de plusieurs maladies graves […] ou très lourdement endetté […].
La délégation a enfin constaté que les mots de passes des étudiants leur permettant d'accéder à leur espace personnel sont générés automatiquement et leur sont adressés en clair dans un courriel sans obligation de modification ni de renouvellement. Dans le cas d'un changement de mot de passe, celui-ci doit être composé de 8 caractères alphanumériques comprenant des lettres majuscules et minuscules.

II- Sur les manquements constatés au regard des dispositions de la loi du 6 janvier 1978 modifiée

*Un manquement à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données*

En premier lieu, s'agissant du dispositif de vidéosurveillance, l'association a indiqué à la délégation de contrôle que le dispositif de vidéosurveillance a été mis en œuvre pour assurer la protection des biens et des personnes, conformément à la déclaration n°1747150 effectuée auprès de la CNIL le 27 février 2014.
La délégation a constaté que les caméras composant le dispositif permettent de visualiser l'ensemble des espaces de travail dédiés aux étudiants (par exemple, la caméra E1-SM-SE ) ainsi que des espaces de pause telle que la cafétéria (par exemple, la caméra KFET-RESTO-SO ) ou encore l'accès aux sanitaires (caméra EO-WC). La délégation a également constaté que certaines caméras permettent de visualiser en continu des postes de travail des salariés (par exemple, la caméra E3-BOCAL ) et les espaces de pauses qui leur sont dédiés (par exemple, la caméra E3-TERRASSE ).
Or, si la CNIL considère de manière constante que des caméras peuvent filmer les accès de l'établissement (entrées et sorties) et les espaces de circulation, il est toutefois exclu de filmer les lieux de vie pendant les heures d'ouverture de l'établissement, sauf circonstances exceptionnelles, non démontrées en l'espèce. De même, le fait de filmer en continu les postes de travail de certains employés est disproportionné, sauf circonstance particulière, par exemple lorsqu'un employé manipule des fonds ou des objets de valeur ou lorsque le responsable de traitement est à même de justifier de vols ou de dégradations commises sur ces zones.

En l'espèce, aucun élément apporté par l'association ne permet de justifier que les étudiants et le personnel soient placés sous surveillance permanente.

En second lieu, l'association a indiqué que les profils des étudiants au sein de la base de données comportent un champ libre qui permet aux membres du personnel de renseigner des informations permettant de justifier les choix pédagogiques effectués pour les étudiants tels que le report d'une période d'examens ou la prolongation de la scolarité. L'association a indiqué qu'aucune procédure quant à l'utilisation de champ libre n'a été mise en place.
La délégation a constaté, dans ces champs libres, la présence de commentaires tels que il a enfin été diagnostiqué de plusieurs maladies graves […], Entre le procès avec son ancien employeur, […]et sa dépression, [X] n'a pas du tout pu se consacrer à 42 , il a à nouveau rechuté dans la dépression , Sa mère a eu un cancer juste avant sa rentrée […] .

Or, l'inscription au sein de la base de données, à laquelle l'ensemble de l'équipe administrative accède, d'informations relatives à l'état de santé de l'étudiant ou à sa situation familiale, apparait disproportionnée au regard de la finalité du traitement, en l'espèce, la gestion pédagogique de l'étudiant.

Il résulte de ce qui précède que l'ensemble de ces faits constitue un manquement aux obligations prévues au 3° de l'article 6 de la loi n°78-17 du 6 janvier 1978 qui dispose que les données à caractère personnel collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs .

*Un manquement à l'obligation de définir une durée de conservation des données proportionnée à la finalité du traitement*

La délégation a été informée qu'aucune durée de conservation n'a été définie par l'association s'agissant des données renseignées par les candidats, qu'ils aient échoué aux tests d'admissibilité ou qu'ils aient intégré l'école.
Tout d'abord, l'association a indiqué que les données concernant les candidats ayant échoué aux tests sont conservées en base active sans limite de temps afin de s'assurer que ces candidats ne puissent plus s'inscrire mais également à des fins statistiques.
S'agissant ensuite des données relatives aux étudiants ayant intégré l'école, l'association a expliqué qu'elles étaient conservées afin de permettre une analyse, à des fins pédagogiques, des différents parcours des étudiants.
Or, la CNIL rappelle que les données à caractère personnel doivent être conservées uniquement le temps nécessaire à l'accomplissement de la finalité qui était poursuivie lors de leur collecte. En l'espèce, si la conservation des données des candidats ayant échoué aux tests apparait légitime, il revient à l'association de s'assurer que seules les données permettant l'identification des candidats soient conservées.
Par ailleurs, la conservation pour une durée indéfinie des comptes des candidats aux tests et des dossiers pédagogiques des étudiants même lorsque ceux-ci ont quitté l'école n'est pas proportionnée à la finalité du traitement, en l'occurrence l'analyse des parcours suivis au sein de l'école.
Ces faits constituent un manquement à l'article 6-5 de la loi du 6 janvier 1978 modifiée, applicable au jour des constats, qui prévoit que les données à caractère personnel sont conservées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

**Un manquement à l'obligation d'informer les personnes**

En premier lieu, s'agissant du dispositif de vidéosurveillance, la délégation a constaté que le règlement intérieur, destiné aux étudiants et aux membres du personnel comporte la mention suivante : Les locaux de L'ECOLE 42 sont placés sous vidéo surveillance. Conformément à la loi n°95-73 du 21 janvier 1995, l'exercice du droit d'accès aux enregistrements vidéo peut s'effectuer auprès de la Direction de l'Etablissement . Par conséquent, les personnes concernées ne sont pas informées des destinataires des données et de la durée de conservation des images. Par ailleurs, l'information délivrée ne vise pas le régime juridique applicable, en l'occurrence la loi Informatiques et Libertés .

En deuxième lieu, la délégation a constaté la présence sur les portes d'entrée de l'école d'autocollants indiquant Etablissement sous vidéo surveillance . Par conséquent, les personnes extérieures à l'école qui seraient amenés à s'y rendre (comme par exemple, un intervenant ou un prestataire) ne sont donc pas informées de l'identité du responsable du traitement, des destinataires, de la durée de conservation des images et des droits dont elles disposent.

En troisième lieu, la délégation a constaté que lors de leur inscription sur le site internet www.42.fr et de leur entrée à l'école, les étudiants sont amenés à renseigner des données personnelles telles que leur nom, leur prénom et leur numéro de téléphone mobile à des fins de gestion administrative et pédagogique de leurs dossiers. Néanmoins, il a été constaté qu'aucune information relative au traitement de leurs données n'est fournie aux étudiants.

Ces faits constituent un manquement au I de l'article 32 de la loi n°78-17 du 6 janvier 1978 modifiée, applicable au jour des constats, qui imposait de fournir à la personne concernée

un certain nombre d'informations quant au traitement de données mis en œuvre et notamment l'identité du responsable de traitement, sa finalité, ses destinataires, l'indication des droit des personnes.

Il est rappelé qu'en application des articles 131-41 et R625-10 du Code pénal combinés, le fait pour la personne morale responsable d'un traitement de ne pas informer, dans les conditions prévues à l'article 32 de la loi du 6 janvier 1978 modifiée, la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est puni d'une peine d'amende pouvant atteindre 7 500 €.

**Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données**

En premier lieu, la délégation a été informée que grâce à une application disponible sur le réseau intranet de l'école, les étudiants ont accès, en temps réel aux images issues des caméras filmant les zones qui leur sont accessibles. Par ailleurs, les membres du personnel administratif ont quant à eux accès, grâce à une autre application, à l'ensemble des images. L'association a indiqué que le dispositif permet aux étudiants de retrouver leurs camarades au sein de l'école et que le choix de leur ouvrir l'accès aux images permet de les rassurer sur ce que visualisent les caméras.

Or, la CNIL considère que l'accès aux images issues du système de vidéosurveillance doit être strictement réservé aux personnes habilitées au regard de leur fonction, par exemple, les agents en charge de la sécurité ou certains membres du personnel administratif. Permettre l'accès aux images issues de la vidéosurveillance à toute personne non habilitée, conduit à compromettre la confidentialité des données traitées.

En deuxième lieu, la délégation a constaté que les mots de passe permettant aux étudiants d'accéder à leur espace personnel sont d'une robustesse insuffisante car composés de 8 caractères alphanumériques comprenant des lettres majuscules et minuscules.

La CNIL rappelle qu'une authentification reposant sur l'utilisation d'un mot de passe insuffisamment complexe peut conduire à une compromission des comptes associés et à des attaques par des tiers non autorisés, par exemple des attaques par force brute qui consistent à tester successivement et de façon systématique de nombreux mots de passe.

En troisième lieu, Ces mots de passe leur sont adressés dans un courriel en clair. Enfin, la délégation a été informée de ce qu'il n'est pas exigé de la part des étudiants la création d'un nouveau mot de passe lors de leur première connexion. Cela implique que dans le cas où l'étudiant ne procède pas lui-même au renouvellement de son mot de passe, celui-ci ne sera jamais renouvelé et restera connu des administrateurs de l'école.

En dernier lieu, l'association a indiqué que les agents de sécurité ont accès au dispositif de vidéosurveillance en utilisant leur propre identifiant associé à un mot de passe de 5 caractères alphanumériques.
L'ensemble de ces mesures ne permet pas au responsable du traitement de s'assurer de la sécurité des données, notamment d'empêcher des tiers non autorisés d'y accéder.

Ces faits constituent donc un manquement à l'article 34 de la loi 78-17 du 6 janvier 1978 modifiée disposant 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 est rappelé qu'en application des articles 226-17 et 131-41 du Code pénal combinés, le fait pour une personne morale de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi 78-17 du 6 janvier 1978 modifiée précitée est puni d'une peine d'amende pouvant atteindre 1 500 000 €.
En conséquence, l'association 42 , sise 96 boulevard de Bessières à Paris (75017), est mis en demeure sous un délai de deux (2) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :
• cesser de traiter des données inadéquates, non pertinentes ou excessives, au regard des finalités poursuivies, conformément aux dispositions du c) de l'article 5 du Règlement (UE) 2016/679 désormais applicable, notamment en :
- modifiant le dispositif de vidéosurveillance afin qu'il soit proportionné au regard de la finalité poursuivie, et en particulier :
*cesser de filmer les espaces de travail des étudiants ainsi que les espaces de pause, cafétérias, et sanitaires pendant les heures d'ouverture de l'école ;
*cesser de placer le personnel administratif sous surveillance constante, par exemple, en réorientant ou en déplaçant les caméras ou encore en procédant à la mise en œuvre de masques dynamiques lors de la visualisation des images.
- prenant des mesures pour éviter que des commentaires excessifs ne soient enregistrés par le personnel administratif dans les profils des étudiants, par exemple, en mettant en place un système de détection automatique de ces derniers et en attirant l'attention du personnel sur la nécessité de n'enregistrer que les données adéquates et pertinentes ;
• définir et mettre en œuvre une politique de durée de conservation des données qui n'excède pas la durée nécessaire aux finalités pour lesquelles ces données sont collectées, conformément à l'article 5-e) du Règlement 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel, en particulier :
- ne conserver parmi les données relatives aux candidats ayant échoués aux tests d'admission, que celles strictement nécessaires à leur identification ;
*ne conserver que les données relatives au suivi administratif et pédagogique des étudiants que durant le temps de leur scolarité et procéder, si nécessaire, à l'archivage de ces données.
*procéder à la purge des données relatives aux étudiants ayant quitté l'établissement;
• procéder à l'information des personnes dont les données sont traitées, conformément aux dispositions des articles 12 et 13 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, désormais applicable, et en particulier :
- s'agissant du dispositif de vidéosurveillance :
*en complétant la mention d'information dans le règlement intérieur en ajoutant notamment l'identité du responsable du traitement, la durée de conservation des données et l'indication des droits des personnes ;
*en complétant le dispositif présent à chacune des entrées de l'école, de l'identité du responsable du traitement, des destinataires des données, de la durée de conservation, des droits dont ils disposent et des modalités d'exercice de ces droits.
- s'agissant de l'inscription des candidats aux tests d'admissions sur le site www.42.fr et des étudiants lors de leur entrée à l'école :
*en fournissant directement aux personnes, au moment où les données à caractère personnel sont collectées sur la page d'inscription, à minima une information relative à

l’identité du responsable du traitement, à la finalité poursuivie par le traitement, aux droits des personnes.
*en complétant cette information, par exemple dans les conditions générales d’utilisation du site www.42.fr et s’agissant des étudiants, au moyen d’une notice d’information, l’ensemble des informations prévues par l’article 13 du Règlement 2016/679.
• prendre toute mesure, pour l’ensemble des traitements de données à caractère personnel mis en œuvre, permettant de préserver la sécurité de ces données et d’empêcher que des tiers non autorisés y aient accès en application de l’article 32 du Règlement (UE) 2016/679 désormais applicable, notamment :
- en s’assurant que les étudiants ne puissent accéder aux images issues du dispositif de vidéosurveillance ;
- en cessant d’adresser dans un courriel en clair leur mot de passe aux étudiants ;
- en obligeant les étudiants à modifier leur mot de passe lors de leur première connexion ;
- en mettant en œuvre une politique de gestion des mots de passe contraignante, s’agissant des postes de travail des agents de sécurité et de l’accès des étudiants à leur espace personnel selon l’une des modalités suivantes ;
*les mots de passe sont composés d’au minimum 12 caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ;
*les mots de passe sont composés d’au moins 8 caractères, contenant 3 des 4 catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s’accompagnent d’une mesure complémentaire comme la temporisation d’accès au compte après plusieurs échecs, (suspension temporaire de l’accès dont la durée augmente à mesure des tentatives), la mise en place d’un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha ) et/ou le blocage du compte après plusieurs tentatives d’authentification infructueuses (au maximum 10).
- prévoir, s’agissant des postes de travail des agents de sécurité, un renouvellement régulier des mots de passe.
À l’issue de ce délai, si l’association 42 s’est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.
À l’inverse, si l’association 42 ne s’est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l’une des sanctions prévues par l’article 45 de la loi du 6 janvier 1978 modifiée.
La Présidente
Isabelle FALQUE-PIERROTIN