

Date de publication sur legifrance: 22/11/2017

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2017-012 du 16 novembre 2017

Délibération de la formation restreinte n° SAN-2017-012 du 16 novembre 2017 prononçant une sanction pécuniaire à l'encontre de la société WEB EDITIONS

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° 2017-015C du 4 janvier 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 des traitements mis en œuvre par la société WEB EDITIONS accessibles à partir des domaines passeport-express.org , formalite-acte-de-naissance.org , porter-plainte.fr , kbis.pro et demande-non-gage.org ;

Vu la décision n° 2017-044C du 27 janvier 2017 de la Présidente de la Commission de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification sur place des traitements mis en œuvre par la société WEB EDITIONS ;

Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur devant la formation restreinte, en date du 22 juin 2017 ;

Vu le rapport de Monsieur Éric PÉRÈS, commissaire rapporteur, notifié par porteur à la société WEB EDITIONS le 4 juillet 2017 ;

Vu les observations écrites de la société WEB EDITIONS reçues le 23 août 2017, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 7 septembre 2017 :

- Monsieur Éric PÉRÈS, Commissaire, en son rapport ;
- En qualité de représentants de la société WEB EDITIONS :
- En qualité de conseils de la société WEB EDITIONS :
- M. X, président ;
- M. Y, directeur général ;
- M. Z ;
- Mme XY ;

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

Les représentants de la société WEB EDITIONS ayant pris la parole en dernier ;

A adopté la décision suivante :

I. Faits et procédure

La société WEB EDITIONS (ci-après la société) est une société par actions simplifiée ayant pour activité principale l'édition de sites internet permettant aux particuliers d'effectuer des démarches administratives en ligne. Elle emploie quatre salariés et a réalisé en 2016 un chiffre d'affaires de 759 758,77 euros.

Le 17 décembre 2016, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a été alertée par l'éditeur d'un site web spécialisé dans la sécurité des systèmes d'information de la découverte d'un incident de sécurité sur les sites www.passeport-express.org , www.formalite-acte-de-naissance.org et www.demande-non-gage.org . Il était indiqué à la CNIL qu'il était possible d'accéder librement aux données renseignées par les utilisateurs sur les formulaires présents sur ces sites internet, sans processus d'authentification.

En application de la décision n° 2017-015C de la Présidente de la Commission du 4 janvier 2017, plusieurs délégations de la CNIL ont procédé à des missions de contrôle en ligne les 11,12 et 13 janvier 2017. Les procès-verbaux de constats n° 2017-015/1, n° 2017-015/2, n° 2017-015/3, n° 2017-015/4 et n° 2017-015/5 dressés à l'issue de ces missions, ont été adressés à la société le 18 janvier 2017.

Au cours des contrôles, les délégations ont suivi le parcours de démarches administratives en renseignant les formulaires présents sur les sites www.passeport-express.org , www.porter-plainte.fr , www.formalite-acte-de-naissance.org , www.demande-non-gage.org et www.kbis.pro . À la fin de chaque démarche, les délégations ont constaté qu'une page récapitulative contenant des données à caractère personnel était affichée ainsi que la présence dans le navigateur des adresses URL suivantes :

<https://www.porter-plainte.fr/DemandeActes/add5/9756>

https://www.passeport-express.org/demande_actes/recap/48423

https://www.formalite-acte-de-naissance.org/demande_actes/recap/436770

<http://www.demande-non-gage.org/DemandeActes/recap/14>

<http://www.kbis.pro/obtenir>

S'agissant des quatre premières adresses URL, les délégations ont constaté qu'en modifiant les derniers numéros, correspondant à l'identifiant attribué à une démarche, les informations renseignées par d'autres utilisateurs du site étaient accessibles. S'agissant du site www.kbis.pro , les vérifications n'ont pas conduit à constater que l'URL contenait un numéro de demande modifiable.

L'absence de système d'authentification des utilisateurs, lors de la démarche en ligne, a ainsi permis à la délégation d'avoir accès notamment aux données d'identification des personnes, ainsi qu'à leur adresse électronique, adresse postale, numéro de téléphone, nom et prénom de leurs parents lorsque la demande portait sur un acte de naissance, ainsi qu'aux descriptifs des faits dans le cadre des dépôts de plainte.

Le 13 janvier 2017, la délégation a pris contact avec la société par courrier électronique (courriel) pour l'informer de l'existence de cette violation de données à caractère personnel. La société a indiqué à la CNIL, par courriel du même jour, qu'elle allait entreprendre les démarches nécessaires. Par courriel du 16 janvier 2017, la société a informé la Commission que le site www.formalite-acte-de-naissance.org avait été modifié afin de protéger les données à caractère personnel des utilisateurs et que les mesures correctrices allaient être répercutées sur les autres sites internet.

La société a indiqué avoir mis en place un système d'authentification lui permettant de s'assurer que la personne accédant à la page récapitulative de la demande était à l'origine de la démarche. Elle a précisé qu'un jeton authentificateur (token) était inséré dans les courriels de confirmation envoyés aux personnes à l'origine des demandes et que celui-ci constituait l'unique moyen d'accéder à la page récapitulative de la demande contenant les données à caractère personnel.

Par courrier du 18 janvier 2017, les procès-verbaux de contrôle en ligne ont été notifiés à

la société. Il lui était également demandé de bien vouloir communiquer à la CNIL le nombre d'utilisateurs présents en base de données pour chaque site internet. La société a fourni à la Commission, par courriel du 30 janvier 2017, les copies du comptage réalisé permettant d'identifier le nombre d'utilisateurs présents en base de données. Il ressortait des pièces communiquées que 9 962 lignes avaient été créées pour le site www.porter-plainte.fr, 148 929 pour le site www.passeport-express.org, 64 867 pour le site www.kbis.pro, 52 018 pour le site demande-non-gage.org et 506 984 pour le site www.formalite-acte-de-naissance.org.

En application de la décision n° 2017-044C du 27 janvier 2017 de la Présidente de la CNIL, une délégation de la Commission a procédé à une mission de contrôle dans les locaux de la société WEB EDITIONS le 6 février 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° 2017-044/1 a été notifié à la société le 9 février 2017.

La société a informé la délégation avoir eu recours, pour éviter la survenance d'un nouvel incident de sécurité, à un cookie fourni par le cadre applicatif CAKEPHP (framework) utilisé pour la conception de ses sites. Elle précisait que ce cookie de session, contenant un identifiant unique, était désormais déposé sur l'équipement terminal de l'utilisateur. Celui-ci permet de s'assurer que la personne souhaitant accéder à une demande pré-enregistrée sur l'un des sites gérés par la société est bien celle qui est à l'origine de la démarche administrative.

La société a également indiqué qu'un utilisateur n'ayant plus le cookie CAKEPHP sur son terminal – en raison d'un changement de poste informatique ou de suppression du cookie – peut accéder à son formulaire grâce au token présent dans le courriel de confirmation qui lui est envoyé.

À l'issue de son instruction, le rapporteur a fait notifier à la société le 4 juillet 2017, par porteur, 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 200.000 euros et qui serait rendue publique.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 7 septembre 2017 indiquant à la société qu'elle disposait d'un délai courant jusqu'au 24 août 2017 pour communiquer ses observations écrites.

Le 23 août 2017, la société WEB EDITIONS a produit des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 7 septembre suivant.

Lors de la séance, la proposition de sanction pécuniaire du rapporteur a été ramenée à la somme de 120.000 euros, au vu des éléments fournis par la société dans ses observations écrites.

II. Motifs de la décision

1. Sur les motifs de nullité de la procédure soulevés par la société

En premier lieu, la société 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 (ci-après la loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée).

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.

La société fait valoir qu'en application de cette disposition, la formation restreinte ne peut prononcer une sanction contre un responsable de traitement sans que celui-ci n'ait été préalablement mis en demeure par la Présidente de la CNIL de faire cesser le manquement constaté.

La société relève, en outre, que le courriel qui lui a été adressé par la CNIL le 13 janvier 2017 par lequel elle l'informait de l'existence d'une violation de données sur ses sites internet ne constitue pas une mise en demeure. Elle précise qu'en tout état de cause, si ce courriel était considéré comme une mise en demeure, aucune sanction ne pourrait être adoptée à son encontre dès lors qu'elle avait apporté les correctifs nécessaires dans un délai de cinq jours ouvrés et s'était ainsi conformée à la mise en demeure adressée par courriel.

La société estime donc que, dans la mesure où le manquement constaté le jour du contrôle pouvait faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure et compte tenu du fait qu'elle y a mis un terme avant qu'une mise en demeure ne lui soit adressée, la procédure de contrôle engagée par la Commission aurait dû être clôturée.

La formation restreinte prend acte de ce que la société a mis fin à la violation de données après les contrôles en ligne de la CNIL, sans qu'une mise en demeure de la Présidente de la Commission ne lui ait été notifiée.

La formation restreinte relève que le I de l'article 45 précité dans sa rédaction issue de la loi pour une République numérique du 7 octobre 2016, vise à permettre la sanction des manquements constatés mais ne pouvant plus faire valablement l'objet d'une mise en demeure, soit que le manquement, de portée ponctuelle, ne puisse être corrigé, soit que la mise en conformité ait été entre-temps opérée sans attendre une mise en demeure. Les faits susceptibles d'être directement sanctionnés peuvent donc correspondre, soit comme en l'espèce à des manquements achevés sans intervention d'une mise en demeure, soit, dans d'autres hypothèses, à la partie passée d'un comportement ultérieurement mis en conformité à la suite d'une mise en demeure.

Le législateur a ainsi entendu permettre à la formation restreinte de la CNIL de prononcer une sanction, notamment pécuniaire, en cas de manquement dûment constaté mais pour lequel une mise en demeure, laquelle ne peut avoir d'effets que pour l'avenir, et non pour le passé, serait sans objet. En effet, dans sa version antérieure à la loi du 7 octobre 2016, seul un avertissement pouvait être prononcé dans ce type d'hypothèse.

Dès lors, la formation restreinte considère que les mesures prises par un responsable de traitement pour faire cesser un manquement constaté, s'ils justifient qu'aucune mise en demeure ne lui soit adressée pour l'avenir, ne la privent pas de la possibilité de prononcer une sanction, dans la mesure où la mise en conformité spontanée du responsable de

traitement n'a pas pour effet de faire disparaître les manquements passés.

En l'espèce, il ressort du courriel reçu le 16 janvier 2017 que la société a pris des mesures correctives visant à faire cesser le manquement constaté lors du contrôle. La formation restreinte considère que le manquement constaté à la date du contrôle ne pouvait plus faire l'objet d'une mise en demeure, qui aurait donc été sans objet. En revanche, ce manquement a bien été dûment constaté, non contesté et a conduit à priver, pendant toute la durée de son existence, les utilisateurs des sites concernés de leur droit à ce que la confidentialité et la sécurité de leurs données soient assurées.

Ainsi, il peut être fait application du dernier alinéa du I de l'article 45 de la loi du 6 janvier 1978 modifiée, permettant à la formation restreinte de prononcer, sans mise en demeure préalable, les sanctions prévues au I.

En second lieu, la société soutient que la décision de la Présidente de la CNIL du 4 janvier 2017 chargeant le secrétaire général *de procéder ou de faire procéder à une mission de vérification auprès de cette société* n'est pas motivée et ne comporte pas la désignation nominative du secrétaire général et de la Présidente.

La société soutient que les procès-verbaux des constatations en ligne ne comportent pas d'ordre du secrétaire général donnant instruction aux agents de la CNIL de procéder aux contrôles et que les copies d'écrans figurant sur les procès-verbaux de contrôle en ligne sont floues.

La société soutient enfin qu'aucun élément du dossier ne permet d'établir que le procureur de la République a été préalablement informé du déroulement d'une mission de contrôle de la CNIL dans ses locaux.

La formation restreinte relève qu'aucune disposition légale n'impose qu'une décision de la Présidente de la CNIL de diligenter un contrôle soit motivée et fasse figurer le nom du secrétaire général. En outre, il ressort des pièces du dossier que contrairement à ce qu'indique la société, la décision de la Présidente de la CNIL du 4 janvier 2017 comporte sa signature, sa qualité ainsi que ses nom et prénom.

Il ressort également des pièces du dossier que la CNIL a transmis à la société, par courrier du 18 janvier 2017, l'ordre de mission signé par le secrétaire général chargeant les agents de procéder aux contrôles en ligne.

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.

2. 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 la société WEB EDITIONS 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 des sites www.passeport-express.org , www.formalite-acte-de-naissance.org , www.porter-plainte.fr et www.demande-non-gage.org , afin notamment que ces données ne soient pas accessibles à des tiers non autorisés.

En défense, la société reconnaît l'existence de l'incident de sécurité constaté mais souligne qu'elle n'a tiré aucun avantage du manquement à la loi Informatique et Libertés et

qu'elle a mis en place des mesures rapides et efficaces afin d'atténuer le dommage. La société considère, en outre, que seul un informaticien expérimenté était en capacité d'accéder aux données des utilisateurs des sites en modifiant un élément chiffré d'une URL.

Elle conteste, en outre, la légitimité de l'éditeur du site à l'origine du signalement de saisir la CNIL de cette violation de données.

Tout d'abord, la formation restreinte considère qu'au titre des pouvoirs que la CNIL tient des dispositions de l'article 11 de la loi du 6 janvier 1978 modifiée, une mission de contrôle peut être diligentée par une délégation de la Commission, indépendamment de l'origine du signalement reçu par elle - qui est sans incidence sur les suites des procédures de contrôle et de sanction - les faits et manquements reprochés se fondant sur les seules constatations effectuées légalement par les agents habilités de la CNIL. Elle note, à cet égard, que les constats de la délégation sont corroborés par la société qui ne conteste pas la survenance d'un incident de sécurité sur ses sites internet.

Ensuite, la formation restreinte relève qu'il est avéré que les services de la CNIL ont pu accéder aux données enregistrées par les utilisateurs des sites

www.passeport-express.org , www.formalite-acte-de-naissance.org , www.porter-plainte.fr et www.demande-non-gage.org .

La formation restreinte note que la modification d'un numéro présent à la fin des URL permettait à des tiers non autorisés d'accéder aux formulaires contenus dans ces pages. Cette violation de données a ainsi été rendue possible par l'absence de mise en place, par la société, d'un dispositif permettant d'éviter la prévisibilité des URL ainsi que d'une procédure d'identification ou d'authentification des utilisateurs.

Or, il ressort des pièces du dossier que la société, disposait, dès l'origine, du dispositif permettant d'assurer la sécurisation des données à caractère personnel des utilisateurs, mais n'a pas jugé utile d'y recourir. Elle était en effet en possession, avec le cadre applicatif CAKEPHP utilisé pour la création de ses sites internet, du cookie identifiant de session mis en place après l'alerte de la CNIL.

En conséquence, il apparaît que le recours à cette solution de sécurisation ne représentait pas un effort disproportionné et était peu coûteuse dès lors qu'elle était disponible dans l'outil utilisé pour la conception de ses sites internet.

La formation restreinte souligne à cet égard que la rapidité des mesures correctrices mises en œuvre par la société illustre la simplicité avec laquelle il était possible d'empêcher la violation de données constatée par la Commission.

La formation restreinte note, en outre, que la violation de données a été réalisée en faisant un usage normal du site, par simple modification des URL, et ne nécessitait aucune compétence technique particulière.

Elle relève enfin que les mesures élémentaires de sécurité n'ont pas été prises par la société. Il ressort du dossier que la société ne s'est pas assurée de l'absence de vulnérabilité de ses sites internet en amont, en vérifiant, par exemple que leur mise en production avait été précédée d'un protocole complet de test. Il apparaît en outre que la société n'a pas procédé, après le déploiement des sites internet, aux vérifications régulières qui lui incombait quant aux mesures de sécurité mises en place.

La formation restreinte estime, par conséquent, que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées.

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 1^{er} et 2^{ème} 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 .

La société soutient que le comptage effectué par le rapporteur du nombre de personnes concernées par la violation de données (717 893) résultant de l'addition du nombre de lignes créées pour chaque site est erroné et surévalué. Elle précise que le rapporteur s'est fondé sur le nombre des pistes créées lorsqu'un internaute commence à remplir un formulaire en ligne, alors que dans certaines hypothèses, il ne deviendra pas utilisateur du service car il n'aura pas finalisé la démarche.

La société relève que la majorité des données rendues accessibles n'étaient pas des données sensibles et que si certaines données relatives à la santé ou à l'intimité des personnes ont pu être accessibles sur le site www.porter-plainte.fr le nombre de données demeure limité dans la mesure où les utilisateurs de ce site ne représentent que 6% de la totalité des utilisateurs des cinq sites de la société.

Elle soutient en outre qu'une sanction d'un montant de 200.000 euros proposée par le rapporteur dans son rapport, serait disproportionnée au regard des critères posés par l'article 47 de la loi du 6 janvier 1978 modifiée dès lors qu'elle n'a tiré aucun avantage du manquement à la loi et qu'elle a mis en place des mesures rapides et efficaces afin d'atténuer le dommage. Elle ajoute qu'une sanction d'un tel montant remettrait en cause sa viabilité.

Le rapporteur a, au cours de la séance, ramené sa proposition de sanction pécuniaire à 120.000 euros.

La formation restreinte considère que la gravité de la violation est constituée en raison de la nature des données concernées.

Elle estime qu'il appartenait à la société, dès lors qu'elle mettait en ligne des sites internet permettant d'effectuer des démarches administratives (www.formalite-acte-de-naissance.org , www.passeport-express.org , www.demande-non-gage.org et www.porter-plainte.fr) d'être vigilante sur la sécurité des données collectées. Elle considère, en effet, que la société WEB EDITIONS ne pouvait s'abstenir, en se positionnant en tant qu'intermédiaire entre les administrés et les services de l'Etat, de placer la sécurisation des données à caractère personnel au cœur de ses préoccupations.

La violation a ainsi rendu accessibles des données d'identification des clients telles que, selon les sites, des noms, prénoms, dates de naissance, coordonnées postales, téléphoniques et électroniques, mais également des données d'identification des parents (noms, prénoms et nom de jeune fille de la mère).

Il apparaît en outre, que certaines données concernées par la violation relèvent de l'intimité de la vie privée des personnes dès lors que celles-ci avaient effectué un récit particulièrement détaillé des faits pour lesquels elles souhaitaient déposer une plainte.

La formation restreinte relève que certaines personnes ont fourni, dans les formulaires du site www.porter-plainte.fr , des informations considérées comme étant des données sensibles au sens de l'article 8 de la loi Informatique et Libertés (*madame S. B., profite de mon état de fragilité physique et psychologique à rapport mon handicap, pour me harceler... , je suis en pleine dépression, je me fais soigner pour une pathologie sévère, j'ai le VIH*) ainsi que des données relatives à des infractions au sens de l'article 9 de la loi précitée. La formation restreinte note que, quand bien même les utilisateurs du site www.porter-plainte.fr ne représenteraient que 6% de la totalité des utilisateurs des sites de

la société WEB EDITIONS, cette proportion représente un nombre important de ses clients.

En outre, la formation restreinte prend acte de ce que la société a communiqué à la délégation de contrôle, au titre du nombre d'utilisateurs présents en base de données, le nombre de pistes créées par les internautes et que dans ces conditions le nombre de 717 893 personnes est incertain. Interrogée en séance sur le nombre réel d'utilisateurs, la société n'a pas été en mesure de renseigner la formation restreinte. Il ressort, cependant, des éléments fournis par la société que les données à caractère personnel d'un nombre important d'utilisateurs, mais aussi de tiers visés dans les formulaires, ont été concernées par l'incident de sécurité.

Par conséquent, la formation restreinte considère que la gravité du manquement commis par la société WEB EDITIONS est caractérisée.

La formation restreinte note, toutefois, que la société a réagi rapidement après avoir eu connaissance de la violation de données en mettant en place des mesures correctrices trois jours après avoir été alertée par la CNIL. Elle prend également acte de ce que la société 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.

La formation restreinte relève enfin que la structure de l'entreprise, composée de seulement quatre salariés, et sa situation financière doivent être prises en compte pour la détermination de la sanction.

Au regard de l'ensemble des éléments précités, une sanction d'un montant de 25.000 (vingt-cinq mille) euros apparaît proportionnée.

La formation restreinte considère qu'au regard du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les internautes quant au risque pesant sur la sécurité de leurs 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 la société WEB EDITIONS une sanction pécuniaire d'un montant de 25.000 (vingt-cinq 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

C
e
t
t
e
d
é
c
i
s
i
o
n
e
s

t
s
u
s
c
c
e
p
t
i
b
l
e
d
e
f
a
i
r
e
f
o
b
j
e
c
t
d
'
u
n
r
e
c
o
u
r
s
d
e
v
a
n
t
l
e
C
o
n
s
e
i
d
'
E

a
t
d
a
n
s
u
n
d
é
l
a
i
d
e
d
e
u
x
m
o
i
s
à
c
o
m
p
t
e
r
d
e
s
a
n
o
t
i
f
i
c
a
t
i
o
n
.

Nature de la délibération: SANCTION