Commission Nationale de l'Informatique et des Libertés
Délibération n°2015-379 du 5 novembre 2015
Délibération de la formation restreinte n° 2015-379 du 5 novembre 2015 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER

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

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 plainte n° 14019869 du 8 juillet 2014 ;

Vu la décision n° 2014-160C du 16 juillet 2014 de la Présidente de la Commission nationale de l'informatique et des libertés ordonnant une mission de vérification auprès de la société OPTICAL CENTER ;

Vu le procès-verbal de contrôle sur place n° 2014-160/1 du 22 juillet 2014 ;

Vu la décision n° 2014-062 du 9 décembre 2014 de la Présidente de la Commission nationale de l'informatique et des libertés de mettre en demeure la société OPTICAL CENTER ;

Vu le procès-verbal de contrôle sur place n° 2014-160/2 du 23 février 2015 ;

Vu le procès-verbal d'audition sur convocation n° 2014-160/3 du 3 juin 2015 ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 25 juin 2015 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, remis à la société OPTICAL CENTER contre reçu le 24 août 2015 ;

Vu les observations écrites versées par la société OPTICAL CENTER le 29 septembre 2015, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier.

Ayant entendu, lors de la séance de la formation restreinte du 6 octobre 2015 :

- Monsieur François PELLEGRINI, commissaire, en son rapport ;

- Madame Catherine POZZO DI BORGO, commissaire du Gouvernement adjoint, n'ayant pas formulé d'observation ;

- Monsieur XXXX de la société OPTICAL CENTER ;
- Madame XXXXde la société OPTICAL CENTER ;
- Maître XXXX, avocat de la société OPTICAL CENTER.

La société OPTICAL CENTER ayant pris la parole en dernier ;

A adopté la décision suivante :

I. Faits et procédure

La société OPTICAL CENTER (ci-après la société) a pour activité la distribution de produits optiques via un réseau d'environ 400 magasins et un site internet (www.optical-center.eu, qui redirige l'internaute vers l'URL www.optical-center.fr et qui compte environ 170.000 comptes utilisateurs). Elle emploie environ 1.000 salariés et présentait en 2014 un chiffre d'affaires d'environ 170 millions d'euros.

Le 8 juillet 2014, la CNIL a été saisie par une plaignante qui dénonçait la communication par téléphone de son mot de passe par la société, laissant ainsi supposer que les mots de passe des comptes clients étaient stockés en clair dans la base de données.

Le 22 juillet 2014, en application de la décision n° 2014-160C du 16 juillet 2014 de la Présidente de la CNIL, il a été procédé à une mission de contrôle auprès de la société au cours de laquelle des manquements à la loi du 6 janvier 1978 modifiée (ci-après loi Informatique et Libertés) ont été constatés.

Par décision n° 2014-062 du 9 décembre 2014 de la Présidente de la CNIL, la société a fait l'objet d'une procédure de mise en demeure lui enjoignant, dans le délai d'un mois, d'adopter des mesures correctives destinées à définir et mettre en œuvre une durée de conservation des données, à informer les personnes concernées des traitements de données opérés et à assurer la sécurité et la confidentialité des données collectées par la société et celles gérées par ses prestataires, et de répercuter ces mesures sur l'ensemble de ses magasins.

La société ayant apporté des éléments attestant d'une mise en conformité partielle, la CNIL a procédé à une nouvelle mission de contrôle, le 23 février 2015. Compte tenu des difficultés rencontrées pour obtenir des informations quant à l'étendue de la mise en conformité, la société a été convoquée, le 3 juin 2015, pour une audition devant la CNIL.
En raison de la persistance de certains manquements, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 25 juin 2015, sur le fondement de l'article 46 de la loi du 6 janvier 1978.

A l'issue de son instruction, le rapporteur a notifié à la société, le 24 août 2015, 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 dont il sollicitait par ailleurs qu'elle soit rendue publique.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 6 octobre 2015 indiquant à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites.
Le 29 septembre 2015, la société a produit des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 6 octobre 2015.

II. Motifs de la décision

1. Sur l'existence d'un manquement à l'obligation de définir et mettre en œuvre une durée de conservation des données

L'article 6-5° de la loi du 6 janvier 1978 modifiée 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.

La société a été mise en demeure de respecter les durées de conservation prévues par les normes simplifiées n° 48 et 54.

Au vu des éléments matériels du dossier, la formation restreinte considère que l'existence d'un manquement à l'article 6-5° de la loi du 6 janvier 1978 modifiée n'est pas caractérisée.

2. Sur l'existence d'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 .

La mise en demeure du 9 décembre 2014 a enjoint à la société de mettre en œuvre un chiffrement du canal de communication et une authentification du site distant lors de l'accès au site web. Or, lors du contrôle du 23 février 2015 et de l'audition du 3 juin 2015, il a été constaté une absence de sécurisation de la page d'accueil permettant à l'utilisateur de se connecter à son compte et de la page lui permettant de modifier son mot de passe.

En outre, la société a été mise en demeure d'améliorer la robustesse des mots de passe de ses clients et salariés. Or, lors du contrôle du 23 février 2015, il a été constaté une absence de complexité suffisante des mots de passe des clients ayant déjà créé un compte. Lors de l'audition du 3 juin 2015, la CNIL a également été informée que la responsable du site web procédait elle-même au changement des mots de passe permettant aux salariés habilités d'accéder au back office et qu'aucun mécanisme de renouvellement automatique n'avait été prévu pour faire face à son absence prolongée. La société n'avait pas non plus défini de politique de gestion des mots de passe pour l'accès aux postes informatiques des salariés.

Enfin, lors de l'audition du 3 juin 2015, la société a précisé que l'accès depuis Internet au back office s'effectuait au moyen d'un couple identifiant et mot de passe, alors même que la mise en demeure imposait une mesure d'authentification forte impliquant de prévoir un second facteur d'authentification de l'utilisateur. De même, alors que la société a été mise en demeure de procéder au verrouillage automatique des postes informatiques des salariés en cas d'inactivité prolongée, seuls 11 postes faisaient l'objet d'un verrouillage automatique.

En défense, si la société ne conteste pas que la page permettant aux utilisateurs de modifier leur mot de passe n'était pas sécurisée, elle soutient que conformément à la mise en demeure, OPTICAL CENTER avait sécurisé toutes les pages contenant des données personnelles.

La société soulève également qu'il lui était impossible de vérifier la modification des mots de passe des clients ayant déjà un compte, ceux-ci étant chiffrés en base. Elle précise que les mots de passe des salariés ayant accès au back office sont dorénavant connus d'eux seuls et que, en l'absence de la responsable du site web, leur renouvellement se fait auprès du prestataire sur demande du directeur commercial de la société. La société ajoute encore avoir mis en place une politique conforme de gestion des mots de passe pout les postes informatiques des salariés.

Enfin, la société soutient que le recours à une mesure d'authentification forte pour accéder au back office du site lui était apparue excessive dans la mesure où les mots de passe des salariés concernés sont dorénavant complexes, et connus d'eux seuls, et que le protocole HTTPS a été mis en place pour la connexion des administrateurs au back office. Elle indique également que le verrouillage automatique de tous les postes informatiques des salariés n'est pas nécessaire dans la mesure où ces derniers disposent de bureaux personnels non accessibles au public.

Au regard de ce qui précède, la formation restreinte relève que le manquement relatif à la sécurisation du site était caractérisé au jour de l'expiration du délai de mise en conformité imparti et persistait au jour du second contrôle. Le fait que le protocole HTTPS est dorénavant en place sur l'ensemble du site est sans incidence sur la caractérisation de ce manquement.

En outre, la formation restreinte considère qu'il suffisait à la société d'imposer à tous ses clients le renouvellement de leur mot de passe pour se mettre en conformité, sans avoir besoin d'y accéder en base pour vérifier leur modification, ce qui aurait été contraire aux prescriptions de la Commission en la matière. S'agissant des mots de passe pour l'accès au back office, la formation restreinte relève que les salariés doivent pouvoir procéder directement à leur renouvellement. Concernant les mots de passe pour les postes informatiques des salariés, elle considère que la sécurisation globale du système d'information ne peut reposer uniquement sur la sécurité physique des locaux, en particulier dans les circonstances de l'espèce où le verrouillage automatique de l'ensemble des postes informatiques des salariés n'était pas assuré. Si la société s'est finalement conformée à la mise en demeure sur la politique de gestion des mots de passe des salariés, le manquement était caractérisé à l'expiration du délai de mise en conformité.

(...)

Le manquement à l'article 34 de la loi du 6 janvier 1978 modifiée est ainsi caractérisé.

3. Sur l'existence d'un manquement à l'obligation d'assurer la sécurité et la confidentialité des données gérées par un sous-traitant.

L'article 35 de la loi n° 78-17 du 6 janvier 1978 dispose, en ses alinéas 3 et 4, que : Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

Lors du contrôle du 22 juillet 2014, il a été constaté que le contrat conclu entre la société et son sous-traitant XXXX ne comportait aucune clause relative à la sécurité et à la confidentialité des données. Il a été enjoint à la société de prévoir une clause définissant les obligations de son prestataire en la matière et précisant que ce prestataire ne pouvait agir que sur son instruction.

En défense, la société a indiqué que l'article 19 du contrat conclu avec la société XXXX était dédié à la sécurité et la confidentialité des données.

La formation restreinte relève que cet article a uniquement trait aux conditions d'accès et de rectification par la société aux données qui la concernent. Il ne comporte aucune indication des obligations incombant au prestataire en matière de protection de la sécurité et de la confidentialité des données des clients de la société.

Enfin, la formation restreinte relève que, contrairement à ce qui lui était demandé, la société n'a pas répercuté les exigences de la mise en demeure sur l'ensemble de ses magasins.

Le manquement à l'article 35 de la loi du 6 janvier 1978 modifiée est ainsi caractérisé.

III. Sur la sanction et la publicité

Les manquements aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée, qui ont persisté au-delà du délai imparti par la mise en demeure de la Présidente de la Commission, justifient le prononcé d'une sanction, notamment en raison du nombre de personnes concernées par les traitements en cause et la sensibilité des données à caractère personnel.

Compte tenu du nombre et de la gravité des manquements de la société, portant sur la sécurité et la confidentialité de données à caractère personnel, la formation restreinte décide de prononcer une sanction pécuniaire de 50 000 euros et de rendre publique sa délibération.

PAR CES MOTIFS :

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

- De prononcer une sanction pécuniaire d'un montant de 50.000 euros à l'encontre de la société OPTICAL CENTER ;

- De rendre publique sa délibération sur le site de la CNIL et sur le site de Légifrance.

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