Délibération CNIL n°SAN-2018-002 du 7 mai 2018

Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 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, de M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA et Monsieur 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 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2011-334 du 29 mars 2011, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 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° 2017-189C du 28 juillet 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 à partir du domaine optical-center.fr ;

Vu la décision n° 2017-197C du 28 juillet 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 OPTICAL CENTER ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 15 décembre 2017 ;

Vu le procès-verbal de constatation en ligne n° 2017-189/1 du 31 juillet 2017 ;

Vu le procès-verbal de contrôle sur place n° 2017-197/1 du 9 août 2017 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, notifié à la société OPTICAL CENTER le 26 décembre 2017 ;

Vu les observations écrites de la société OPTICAL CENTER reçues le 6 février 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 22 février 2018 :

- M. François PELLEGRINI, Commissaire, en son rapport ;

En qualité de représentants de la société OPTICAL CENTER :

- X ;
- Y ;
- Z ;

En qualité de conseil de la société OPTICAL CENTER :

- XY.

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

Les représentants de la société OTPICAL CENTER ayant pris la parole en dernier ;

A adopté la décision suivante :

1. Faits et procédure

La société OPTICAL CENTER (ci-après la société) est spécialisée dans le commerce de détail d'optique. Elle dispose à cet effet d'une centaine de succursales, d'un réseau de 410 franchises et d'un site internet (www.optical-center.fr). Elle présentait pour l'année 2016 un chiffre d'affaires consolidé d'environ 193 millions d'euros, le chiffre d'affaires généré par son site internet s'élevant à près de 4,25 millions d'euros.

Le 28 juillet 2017, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été informée d'une possible fuite de données concernant la société OPTICAL CENTER. Ce signalement faisait état de données à caractère personnel rendues librement accessibles à partir de plusieurs URL ayant une structure identique.

Le 31 juillet 2017, en application de la décision n° 2017-189C de la Présidente de la Commission, une délégation de la CNIL a effectué des vérifications en ligne qui ont permis de constater qu'il était possible d'accéder librement, à partir des URL qui lui avaient été transmises, à plusieurs factures contenant les données à caractère personnel suivantes : nom, prénom, adresse postale, correction ophtalmologique et, pour certaines d'entre elles, la date de naissance des clients ainsi que leur numéro d'inscription au répertoire national d'identification des personnes physiques (NIR).

La délégation a également constaté qu'il était possible, depuis le domaine optical-center.fr et sans authentification préalable à l'espace client, d'exporter au format CSV, un échantillon de 2085 fichiers correspondant, après dédoublonnage, aux données de […] clients et faisant notamment apparaître 158 NIR.

La société OPTICAL CENTER a été alertée le jour même, par un courrier électronique de la Commission lui indiquant qu'il était possible d'accéder à des pages présentant des données à caractère personnel depuis un navigateur, sans autorisation particulière.

Lors d'une seconde mission de contrôle effectuée le 9 août 2017 dans les locaux de la société OPTICAL CENTER, la délégation de la CNIL a été informée que les factures et les bons de commande rendus librement accessibles correspondaient uniquement aux commandes effectuées sur le site internet de la société. Le responsable de ce site a précisé que le défaut de sécurisation était dû à *l'absence de contrôle de la connexion d'un client avant l'affichage de leur contenu* .

La délégation a également été informée par le prestataire de la société OPTICAL CENTER que la correction du défaut de sécurité affectant le site internet avait été réalisée le 2 août 2017, à la suite du contrôle en ligne opéré par la délégation de la CNIL. En l'espèce, une fonctionnalité a été ajoutée afin de s'assurer qu'un client est effectivement *connecté* à son espace personnel avant de lui fournir les seuls documents le concernant.

Lors du contrôle sur place du 9 août 2017, la délégation a constaté qu'il n'était effectivement plus possible d'accéder aux factures accessibles à partir des URL litigieuses. Elle a également été informée que ni la société OPTICAL CENTER, ni son prestataire n'avaient eu connaissance du défaut de sécurité avant que celui-ci n'ait été porté à leur connaissance par la CNIL le 31 juillet 2017.

Interrogée sur la date à laquelle le défaut de sécurité était apparu en production, la société a indiqué ne pas en avoir connaissance. Par courrier du 7 septembre 2017, elle a cependant indiqué que la mise en production du code permettant la visualisation des URL signalées au 31 juillet 2017 datait de décembre 2016.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 15 décembre 2017, 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).

A l'issue de son instruction, le rapporteur a notifié à la société OPTICAL CENTER, par porteur, le 26 décembre 2017, 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 d'un montant qui ne saurait être inférieur à deux cents cinquante mille (250.000) euros et de la rendre publique.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 22 février 2018 indiquant à l'organisme qu'il disposait d'un délai courant jusqu'au 5 février 2018 pour communiquer ses observations écrites.

Par courrier du 2 février 2018, la société OPTICAL CENTER a produit des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 22 février 2018. Le 5 mars 2018, la société a transmis à la CNIL une pièce complémentaire relative à un programme de protection qui serait mis en œuvre sur son site internet et intitulé *Bannir les activités anormales sur le site* .

1. 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 premier alinéa 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 loi pour une République numérique) ainsi que l'article 59 de la délibération
n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la CNIL.

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'article 59 de la délibération n° 2013-175 précitée énonce que :

Les décisions de mises en demeure adoptées par le président de la Commission, sont signées par le président, ou, en cas d'empêchement, par le vice-président délégué. Elles sont numérotées avec l'indication de l'année en cours et portent la date du jour de leur signature.

Elles caractérisent les manquements reprochés au responsable de traitement et précisent le délai imparti à celui-ci pour se mettre en conformité. Elles indiquent les conséquences pour le responsable du non-respect de la mise en demeure.

La société considère qu'il n'est pas possible de prononcer une sanction à son encontre dès lors qu'elle n'a fait l'objet d'aucune mise en demeure préalable, laquelle constitue une formalité substantielle de la procédure qui concourt au respect des droits de la défense du responsable de traitement. Elle souligne également qu'en l'espèce, le manquement constaté par la CNIL pouvait faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure.

La société estime donc que la Présidente de la CNIL aurait dû la mettre en demeure de corriger le manquement 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 des dispositions du I de l'article 45 de la loi du 6 janvier 1978 modifiée.

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.

La formation restreinte relève enfin que l'article 59 du règlement intérieur de la CNIL dont se prévaut la société se borne à décrire le formalisme qui caractérise les mises en demeure adoptées par le Président de la CNIL, sans qu'aucune conséquence ne puisse en être tirée sur la procédure de sanction.

En second lieu, la société considère que l'extrapolation du nombre de clients et de données concernés par la faille de sécurité effectuée par le rapporteur à partir de l'échantillon des 2075 fichiers téléchargés par la délégation de contrôle porte atteinte aux droits de la défense, sans autre précision. Elle estime à ce titre *ne pas être en mesure de se défendre sur l'ensemble des pièces qui lui est opposé* et, *a fortiori*, être dans l'impossibilité de démontrer le caractère disproportionné de la sanction proposée ce qui serait de nature, selon la société, à entraîner la nullité de la procédure.

La formation restreinte relève que l'estimation à laquelle s'est livré le rapporteur avait pour seul objet de déterminer un ordre de grandeur quant aux données concernées par l'incident de sécurité, en particulier celles relatives aux données sensibles et au NIR. Elle relève également que s'agissant du nombre de clients concernés par l'incident de sécurité et du nombre de documents contenus en base à la date de cet incident, le rapporteur s'est appuyé sur les éléments communiqués par la société dans son courrier du 7 septembre 2017.

En tout état de cause, la formation restreinte rappelle que l'ensemble des éléments sur lesquels le rapporteur s'est appuyé pour établir son rapport a été communiqué à la société. Elle rappelle également que la société avait la possibilité de consulter le dossier dans les locaux de la CNIL, ce qu'elle n'a pas fait, et qu'elle bénéficiait, pour présenter ses observations, d'un délai supérieur au délai d'un mois fixé par l'article 75 du décret n° 2005-1309 du 20 octobre 2005.

Par conséquent, la formation restreinte considère que les moyens tirés de la nullité de la procédure de sanction invoqués par la société doivent être écartés.

1. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données

L'article 34 de la loi du 6 janvier 1978 modifiée dispose que *le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* .

Il appartient à la formation restreinte de décider si la société OPTICAL CENTER 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 enregistrées par le biais de son site internet www.optical-center.fr , notamment afin que ces données ne soient pas accessibles à des tiers non autorisés.

En premier lieu, la société OPTICAL CENTER reconnaît l'existence d'un défaut de sécurité affectant son site internet mais souligne que des précautions ont néanmoins été prises. En particulier, la société détaille les mesures de protection mises en œuvre par elle ainsi que par son prestataire.

À cet égard, la formation restreinte relève tout d'abord que, lors de la séance du 22 février 2018, la société a, en plus des observations présentées à l'appui de ses conclusions écrites, fait état d'un nouvel argument en présentant une nouvelle mesure de sécurité mise en œuvre sur son site internet. Elle a en effet affirmé qu'il aurait été impossible pour la délégation de la CNIL de procéder au téléchargement de sa base de données dans son intégralité dès lors qu'un programme de protection spécifique était mis en place et donc, ***a fortiori***, pour tout individu de télécharger l'ensemble des documents enregistrés sur le site internet de la société. Au soutien de cet argument, la société a transmis, par courrier du 5 mars 2018 et reçu le 12 mars, une pièce intitulée ***Programme de protection Bannir les activités anormales sur le site*** .

La formation restreinte relève que la société n'a jamais mentionné l'existence d'un tel programme tout au long de la procédure alors même que le procès-verbal de constatation en ligne du 31 juillet 2017 faisait expressément état, à deux reprises, du début de l'exécution du script par la délégation de contrôle et de son interruption, à l'initiative de la CNIL.

Sur le fond, elle constate à cet égard que les termes employés dans le procès-verbal de contrôle en ligne sont sans ambiguïté : ***Mentionnons débuter l'exécution du script à 13h06 et l'interrompre à 14h22*** ou encore ***Mentionnons débuter l'exécution du script à 14h47 et l'interrompre à 14h51*** . La formation restreinte constate qu'il n'est nullement mentionné que la délégation de contrôle aurait été mise dans l'impossibilité de télécharger une partie des fichiers contenus dans la base de données de la société : l'exécution du script a été interrompue à l'initiative de la délégation de contrôle. La formation restreinte souligne enfin que l'analyse de la pièce transmise, datée du 26 février 2018, ne permet pas d'attester que le programme ***Bannir les activités anormales sur le site*** était effectivement mis en œuvre antérieurement aux différents contrôles menés par la délégation de la CNIL.

En conséquence, la formation restreinte estime que l'existence du dispositif de protection allégué à la date des faits constatés n'est pas établie au vu des éléments transmis.

Elle relève par ailleurs que, dans le cadre de ses observations écrites, la société a également transmis un document de son prestataire décrivant notamment le processus appliqué lorsqu'un nouveau développement du site est mis en production. Elle explique que de nombreux échanges interviennent avec son prestataire quand bien même aucun document formel n'a été remis à la délégation de la CNIL.

La formation restreinte, tout en soulignant la diligence de la société qui a réagi immédiatement après la révélation de la faille pour corriger cette dernière, relève toutefois que les mesures élémentaires de sécurité n'avaient pas été prises en amont de la mise en production d'une nouvelle fonctionnalité de son site internet.

Elle note à cet égard que le site internet de la société, qui permet d'effectuer des commandes en ligne après avoir créé un compte dédié, n'intégrait pas de fonctionnalité permettant de vérifier qu'un client s'est bien authentifié à son espace personnel avant de lui donner accès auxdits documents. La formation restreinte estime que la société aurait dû mettre en place une restriction d'accès aux documents mis à disposition des clients ***via*** leur espace réservé dès lors que ce dernier a précisément pour objet de permettre aux clients d'accéder aux commandes en cours et passées, à leurs avoirs ou encore à leurs factures. Elle considère ainsi que la mise en place d'une telle fonctionnalité constitue une précaution d'usage essentielle dont la mise en œuvre aurait permis de réduire significativement le risque de survenance d'une telle violation de données.

La formation restreinte relève par ailleurs 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 paramètre id relatif à l'identifiant de la facture, lequel était parfaitement visible au sein de l'URL affichée dans la barre d'adresse du navigateur lorsqu'un client consulte une facture ou un bon de commande. La formation restreinte rappelle en outre que, de manière générale, l'exposition de ressources sans contrôle d'accès préalable, est identifiée depuis de nombreuses années comme faisant partie des failles de sécurité devant faire l'objet d'une surveillance particulière et doit, en conséquence, faire l'objet de vérifications notamment dans le cadre d'audits de sécurité. A cet égard, la formation restreinte souligne la facilité avec laquelle il est possible de

modifier le paramètre d'une URL ainsi que l'importance de procéder à un protocole complet de test en amont de la mise en production d'un site internet.

Elle relève en outre que le caractère informel des échanges qui interviennent entre la société et son prestataire a rendu, en l'espèce, plus difficile le suivi par le responsable de traitement, des actions entreprises par son prestataire, des correctifs apportés par ce dernier ainsi que des recommandations qui pourraient être formulées.

La formation restreinte note par ailleurs que si la société a indiqué, lors de la séance du 22 février 2018, qu'une procédure spécifique était appliquée lors de la mise en production d'une mise à jour de son site internet, une information contraire a été donnée à la délégation de la CNIL lors du contrôle du 9 août 2017. La formation restreinte relève en effet que la société a indiqué qu'il n'existait, au jour du contrôle, aucune procédure décrivant les tests à mettre en œuvre lors d'une mise en production d'une mise à jour du site et qu'aucun procès-verbal de recette n'est établi à cette occasion.

En outre, s'agissant des précautions prises par la société, elle observe notamment qu'aucun élément n'a été transmis permettant d'attester qu'un audit de son site internet ait effectivement été réalisé et, *a fortiori*, qu'un audit du code source dudit site ait déjà été mené. La formation restreinte constate enfin que le document transmis par la société, dans le cadre de ses observations en défense, ne permet pas d'affirmer que les mesures de sécurité élémentaires et correspondant à l'état de l'art étaient effectivement mises en place à la date de l'incident de sécurité.

En deuxième lieu, la société estime que le rapporteur s'est fondé sur des faits inexacts, à savoir le numéro de la dernière facture téléchargée, pour déterminer le nombre de documents ayant été rendu librement accessibles. Elle émet également plusieurs réserves sur la méthodologie employée par le rapporteur pour déterminer le volume de données en cause ainsi que la durée de l'incident.

En ce qui concerne le nombre de documents concernés, la formation restreinte rappelle que c'est la société qui a expressément indiqué, par courrier du 7 septembre 2017, qu'à la date du 31 juillet 2017 sa base de données contenait 299 983 factures et 34 786 bons de commande, soit 334 769 documents. Dès lors que la dernière facture téléchargée par la Commission portait le numéro 354 806 et que, lors du contrôle du 9 août 2017, la société a indiqué que le numéro de facture est notamment constitué d'un numéro de séquence incrémentiel, elle en déduit que la base de données du site internet de la société contenait entre 334 769 et 354 806 documents.

Elle relève que, si la société soutient qu'en réalité seul un nombre limité de factures étaient concernées par l'incident de sécurité, cette dernière ne fournit aucun élément à l'appui de cet argument.

La formation restreinte relève par ailleurs que l'estimation du rapporteur quant au volume de données concernées par l'incident de sécurité résulte de l'analyse de l'échantillon de fichiers téléchargés par la délégation de la CNIL lors du contrôle du 31 juillet 2017. Elle considère qu'une telle estimation avait pour objet de déterminer un ordre de grandeur quant aux données ayant été rendues librement accessibles dès lors que la société n'a été en mesure d'indiquer ni le nombre de clients uniques concernés par l'incident de sécurité, ni le nombre de numéros de sécurité sociale ayant été diffusés.

La formation restreinte rappelle à cet égard que, si la société a indiqué qu'une telle *extrapolation* à partir d'un échantillon de données *a déjà été écartée par le Conseil d'Etat en matière de contrôle de la sécurité sociale* , aucune autre précision n'a été apportée sur ce point. Or, le Conseil d'Etat a, au contraire, estimé dans une décision du 19 mai 2017 qu'il était possible pour la commission des sanctions de l'Autorité des Marchés Financiers (AMF), compte tenu de la nature du manquement en cause – dans ce cas d'espèce, une manipulation de cours au moyen d'un programme algorithmique appliquant une même stratégie pendant une certaine période - de procéder à une estimation du montant total des profits réalisés *en se fondant seulement sur un échantillon des opérations réalisées* (CE, 19 mai 2017, *req. n° 396698*). De même, la nature du manquement permettait en l'espèce, en tout état de cause, de se fonder sur un échantillon pour en apprécier l'ampleur.

En outre, la formation restreinte rappelle qu'il n'est pas contesté que des données sensibles au sens de l'article 8 de la loi du 6 janvier 1978 modifiée (correction ophtalmologique) ont été rendues librement accessibles sur internet ainsi que le NIR. Elle rappelle qu'il s'agit d'informations relevant de la vie privée des personnes et qui, au regard de leur nature particulière, auraient dû faire l'objet de garanties de sécurité renforcées indépendamment du volume de données concernées.

La formation restreinte relève en outre que tout en s'opposant aux conclusions du rapporteur qui estime que l'incident de sécurité aurait duré près de sept mois sans que la société n'en ait eu connaissance, compte tenu des informations transmises par elle, cette dernière a indiqué à plusieurs reprises ne pas être en mesure de déterminer la date d'apparition de la faille, dont elle a été informée par la CNIL le 31 juillet 2017.

Sur la base de ces éléments, la formation restreinte considère que le manquement à l'article 34 de la loi du 6 janvier 1978 modifié est constitué dès lors que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées.

1. Sur la sanction et la publicité

Aux termes des alinéas 1 er et 2 ème 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 estime qu'au regard des critères fixés par l'article 47 de la loi du 6 janvier 1978 modifiée, le montant d'au moins deux cents cinquante mille (250.000) euros proposé par le rapporteur est disproportionné.

Elle rappelle qu'elle n'a tiré aucun avantage du manquement, lequel est en tout état de cause d'une gravité relative et présente un caractère limité. La société précise que le manquement n'était pas intentionnel et qu'aucun dommage ne semble avoir été subi par les personnes concernées. Elle précise à cet égard, d'une part, qu'il n'était pas possible d'accéder à l'espace client ni de modifier les factures des personnes concernées et, d'autre part, n'avoir trouvé aucune trace d'exploitation desdites données, celles-ci n'ayant par ailleurs pas fait l'objet d'une indexation par les moteurs de recherche.

La société rappelle qu'elle a été extrêmement réactive en informant immédiatement son prestataire de la violation de données, lequel a sans délai procédé à la mise en place d'un correctif. Elle rappelle également avoir coopéré avec la CNIL tout au long de la procédure.

La société fait en outre valoir que le montant de la sanction proposée par le rapporteur tient compte de la précédente sanction prononcée par la formation restreinte à son encontre.

Si la société a fait preuve de réactivité et a effectué les diligences nécessaires auprès de son prestataire, la formation restreinte souligne néanmoins que les services de la CNIL ont pu accéder aux données des clients de la société, cet accès ayant confirmé l'existence du défaut de sécurisation signalé par un tiers. Elle rappelle en outre que la société a reconnu que son site internet présentait un défaut de sécurisation résultant de l'absence de fonctionnalité permettant de vérifier qu'un client s'est bien authentifié à son espace personnel avant de lui permettre l'accès aux factures et bons de commande le concernant. La formation restreinte rappelle à cet égard que la seule modification du code source du site internet a permis de remédier au défaut de sécurisation en cause dont le caractère élémentaire n'a au demeurant pas été contesté.

Elle relève également qu'à la date de l'incident de sécurité, la base de données de la société contenait 334 769 documents et que le défaut de sécurisation a rendu librement accessibles des données directement identifiantes (nom, prénom, adresse postale, date de naissance), des données sensibles au sens de l'article 8 de la loi du 6 janvier 1978 modifiée ainsi que le NIR des personnes concernées. En outre, il a concerné un nombre important de ses clients, la société ayant indiqué que […] clients ont au moins une facture stockée sur son site internet. Rien n'indique par ailleurs qu'à défaut d'avoir été alertée par la délégation de la CNIL, la société aurait eu connaissance de cette violation de données.

La formation restreinte note également que la société se prévaut de l'absence de préjudice pour les personnes concernées par le défaut de sécurité, en indiquant notamment que les URL en cause n'ont pas fait l'objet d'une indexation par les moteurs de recherche. La formation restreinte rappelle toutefois que les risques liés à la divulgation de données personnelles ne sauraient être limités à une indexation de ces dernières par les moteurs de recherche ou à l'accès à l'espace client et à la modification de documents. En effet, la divulgation de données se rapportant à l'identité des personnes concernées expose ces dernières à des risques multiples parmi lesquels figure celui de faire l'objet d'un hameçonnage ciblé (phishing).

En ce qui concerne l'argument de la société tiré de la prise en compte, par le rapporteur, d'une sanction antérieure, la formation restreinte relève que si cet élément a été évoqué par lui, il était présenté comme une simple référence à des fins contextuelles et non comme une circonstance aggravante au titre du manquement qui lui était imputé.

La formation restreinte estime que les termes de l'article 47 de la loi du 6 janvier 1978 ne font au demeurant pas obstacle par eux-mêmes à la prise en compte d'un précédent manquement aux mêmes dispositions de l'article 34 de cette loi, concernant le même site, afin de déterminer le montant de la sanction pécuniaire.

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 deux cent cinquante mille (250.000) euros.

Enfin, elle considère qu'au regard des éléments précités faisant notamment état du caractère particulièrement sensible des données en cause, du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les internautes quant aux risques 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 OPTICAL CENTER une sanction pécuniaire d'un montant de deux cent cinquante mille (250.000) euros ;
- de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.