Délibération de la formation restreinte n° 2015-005 du 25 juillet 2016 prononçant un avertissement à l'encontre de « *New Age Telecom* »

La Commission nationale de l'informatique et des libertés, réunies en sa formation restreinte.

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 la délibération le règlement intérieur de la commission nationale de l'informatique et des libertés ;

Vu les autres pièces du dossier ;

Ayant entendu, lors de la séance de la formation restreinte du 15 juillet 2016 les représentants de la société *New Age Telecom*.

A adopté la décision suivante :

I- Faits et procédure

Le 20 mai 2016, et en application de l'article 34 bis de la loi du 6 janvier 1978 modifiée, la Société *New Age Telecom* (ci-après « la société ») a notifié à la commission nationale de l'informatique et des libertés (ci-après « la Cnil ») une violation de données à caractère personnel ayant impacté environ 655 000 de ses clients.

Celle-ci est intervenue à la suite d'une intrusion dans les serveurs du prestataire de la société chargé d'héberger certaines de ses données.

La société *New Age Telecom* a informé ses clients de cette fuite de données par mail en les prévenant contre les tentatives de phishing.

Sur décision de la présidente de la Cnil, des missions de contrôle dans les locaux de la société et de ceux de son sous-traitant hébergeant certaines de ces données ont été effectuées par une délégation de la Cnil (ci-après « la délégation ») les 05 et 10 juin 2016.

S'agissant de la violation de données personnelles, la délégation a noté que la société *New Age Telecom* a été informée par son prestataire de service d'hébergement et par le message d'un groupe de pirates russes le 20 mai 2016. Le groupe de pirates revendiquait le vol de près de 2 000 000 de données clients de la société *New Age Telecom*. Il a été relevé également que la société avait reçu des plaintes de ses clients par rapport à des phishing, suivis de prélèvements indus sur leurs comptes bancaires.

S'agissant des mesures de sécurité, il a été relevé par la délégation que le mot de passe permettant d'accéder aux serveurs du prestataire de service d'hébergement était composé d'une suite logique de chiffres et de lettres ne garantissant pas une sécurité des informations hébergées.

Il a été noté enfin que si la société avait prévu de façon contractuelle un audit du système d'information de son prestataire de service d'hébergement, cet audit n'a jamais été effectué par elle.

Au regard de ces éléments, la présidente de la Cnil a décidé d'initier une procédure de sanction à l'encontre de la société *New Age Telecom*, et de désigner un commissaire rapporteur sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée.

A l'issue de son instruction, considérant que la société avait manqué à l'obligation de sécurité lui incombant en application de l'article 34 de la loi du 6 janvier 1978 modifiée, le commissaire rapporteur

a notifié à la société, le 28 juin 2016 un rapport proposant à la formation restreinte de la Cnil de prononcer à son encontre un avertissement public.

Suite aux observations écrites produites par la société *New Age Telecom*, réitérées à l'orale à la séance de la formation restreinte de la Cnil du 15 juillet 2016, la formation restreinte a adopté la décision suivante.

II- Motifs de la décision

Concernant l'obligation incombant à la société de mettre en œuvre des moyens propres à assurer la sécurité des données de ses clients notamment pour que ces données ne soient pas communiquées à tiers non autorisés, 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. »

En défense, la société soutient avoir tout mis en œuvre afin de respecter son obligation et soutient que la faille de sécurité serait imputable à son sous-traitant.

La formation restreinte retient qu'en sa qualité de responsable de traitements, l'obligation d'assurer la sécurité et la confidentialité des données à caractère personnel de ses clients lui incombe personnellement et qu'elle ne saurait minimiser sa responsabilité par le recours à des prestataires. Par ailleurs, il a été relevé que le mot de passe de sécurisation de l'ensemble du réseau du quartier par défaut « 123456Digiteco », ne permet pas d'assurer la sécurité et la confidentialité des données aux quelles il permet d'accéder.

Enfin, il ressort des contrôles de la délégation que la société n'a pas fait réaliser d'audit de sécurité du système d'hébergement de données utilisé par son prestataire.

La formation restreinte relève que les mesures mises en œuvre en termes de sécurité des données par la société avant les améliorations apportées suite à la violation de données étaient insuffisantes et ont contribué à la réalisation du risque que constitue la récupération, par un tiers malveillant, des données des clients. Malgré les engagements de la société à assurer une meilleure protection des données de ses clients, il reste indiscutable qu'elle a manqué à son obligation d'assurer la sécurité et la confidentialité des données à caractère personnel de ses clients.

Sur la base de ces éléments, la formation restreinte retient que la société n'a pas respecté les dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

III- Sur la sanction et la publicité

La formation restreinte considère que la société a manqué aux obligations lui incombant en application des dispositions susvisés de la loi du 6 janvier 1978 modifiée et décide de prononcer à son encontre un avertissement en application de l'article 45 de la loi n°78-17 du 6 janvier 1978 modifiée.

Par ailleurs, la formation restreinte décide de rendre publique sa décision.

Par ces motifs

La formation restreinte de la Cnil, après avoir délibéré, décide :

- De prononcer un avertissement à l'encontre de la société *New Age Telecom* ;
- De rendre publique sa décision sur le site Internet de la Cnil,

La présidente.