CNIL

Délibération de la formation restreinte n°2014-238 du 12 juin 2014 prononçant un avertissement rendu public à l'encontre de la société DHL INTERNATIONAL EXPRESS FRANCE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Présidente, M. Alexandre LINDEN, Vice-président, Mme Marie-Hélène MITJAVILE, M. Sébastien HUYGUES 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 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 46 ;

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° 2014-055C du 18 février 2014 de la Présidente de la Commission nationale de l'informatique et des libertés ordonnant une mission de vérification auprès de la société DHL International Express France ;

Vu le rapport de Marie-France MAZARS, commissaire rapporteur, adressé par porteur à la société DHL International Express France, le 12 mars 2014;

Vu les observations écrites versées par la société DHL International Express France le 11 avril 2014, 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 17 avril 2014 se tenant à huis-clos :

- Mme Marie-France MAZARS, Vice-présidente, en son rapport ;
- Mme Catherine POZZO DI BORGO, commissaire du Gouvernement adjoint, en ses observations ;
- M. de la société DHL International Express France, Mc et Me , ses conseils

A adopté la décision suivante :

I. FAITS ET PROCEDURE

La société DHL International Express France (ci-après « la société ») exerce une activité de transport, de logistique et de fret.

Alertée d'une possible faille de sécurité sur les sites internet de la société, la présidente de la Commission nationale de l'informatique et des libertés (ci-après « la CNIL ») a ordonné une mission de contrôle dans les locaux de la société qui s'est déroulée le 19 février 2014. Les constatations effectuées le 19 février 2014 sur les sites internet http://www.dhl.com et http://www.dhl-france.com ont mis en évidence que 684 778 fiches de clients étaient référencées dans un moteur de recherche et pouvaient être directement consultées depuis un ordinateur connecté au réseau internet.

Les fiches librement accessibles sur internet comportaient des données relatives à l'identité, à l'adresse des personnes, à leurs numéros de téléphone et adresses électroniques ainsi que parfois des instructions détaillées de livraison. Il a été reconnu par la société qu'elle était informée de la faille de sécurité depuis la fin de l'année 2013 et qu'une version corrective serait déployée en mars 2014. Il a été également constaté que les fiches les plus anciennes étaient datées de l'année 2007. Ces éléments ont été établis par constat contradictoire.

Par courriel du 28 février 2014 la société à informé la CNIL de la mise en œuvre d'une procédure de suppression de l'accès aux fiches antérieures au 1er février, de la limitation de la durée de conservation des fiches à un mois et de la désindexation des fiches clients du moteur de recherche de la société Google.

Sur la foi de ces éléments, la présidente de la Commission a désigné comme rapporteur Marie-France MAZARS, 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 plusieurs obligations lui incombant en application de la loi du 6 janvier 1978 modifiée, le rapporteur a notifié, par porteur à la société le 12 mars 2014, 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 à l'encontre de la société un avertissement, dont il sollicitait par ailleurs qu'il soit rendu public.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 17 avril 2014 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites.

La société a produit, par courrier daté du 11 avril 2014, des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte tenue à huis-clos le 17 avril 2014.

A l'issue de cette procédure, et après en avoir délibéré, la formation restreinte a adopté la décision dont la teneur suit.

II. MOTIFS DE LA DECISION

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 a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données de ses clients

et notamment des mesures adaptées pour que ces données ne soient pas communiquées à des tiers non autorisés.

Il ressort du procès-verbal de contrôle, sans que cela soit contesté, que plusieurs centaines de milliers de fiches comportant des données à caractère personnel relatives aux clients de la société étaient indexées et librement consultables sur internet sans manipulation technique particulière. Il est également établi que ces données issues de la base de données « avis de passage » étaient de natures diverses et que certaines présentaient un réel caractère d'intimité, révélant des éléments relatifs à la santé des personnes ou relatives à la sécurisation des accès aux logements des clients.

En défense la société conteste avoir eu connaissance du défaut de sécurisation de son site internet avant la date du contrôle et ceci en contradiction avec les déclarations portées au procès verbal de contrôle. Elle explique que la mention de la connaissance d'une faille relative à la base de données « avis de passage » était relative à un défaut de sécurisation des accès internes à l'application et non des accès externes. Le salarié présent lors du contrôle aurait donc à tort signé le procès-verbal de contrôle sans émettre de réserves.

La société fait valoir que dès la connaissance de la faille à l'issue du contrôle, elle a mis en œuvre les procédures nécessaires à la sécurisation de l'accès aux fiches et à la suppression des fiches datant de plus d'un mois. Elle estime ainsi démontrer sa bonne foi et son absence de négligence vis-à-vis des obligations lui incombant au titre de l'article 34 précité. Au surplus, elle indique que sa réponse a été rapide et sa coopération complète. Concernant le défaut de sécurisation des accès internes, elle avait indiqué avoir programmé une migration vers une nouvelle application pour le mois de mars 2014 dont elle confirme la réalisation.

Pour expliquer l'origine de la faille de sécurité, la société indique que l'application dont il est discuté a été conçue il y a plusieurs années par un sous traitant et que l'absence de mesure de sécurisation constatée au niveau de l'adresse IP résulte d'un défaut de conception du design de l'application. Elle entend cependant assurer la formation restreinte de sa parfaite prise en compte des questions de sécurité informatique et de protection des données personnelles. A cet égard, elle fait valoir la désignation d'un correspondant informatique et libertés avant la découverte de la faille, l'existence d'une politique globale de sécurité pour la société et des actions de sensibilisation à ces questions ainsi que l'accompagnement par un cabinet labélisé par la CNIL.

Ces éléments rappelés, la formation restreinte, sur la base des éléments du constat non démentis, constate que jusqu'à une date récente et depuis un temps indéterminé, de nombreuses données à caractère personnel relatives aux clients de la société étaient indexées et accessibles à tous sur internet sans compétence technique particulière.

Elle constate que cette situation résulte d'un défaut dans la conception dont la responsabilité incombe nécessairement à la société en tant que responsable de traitement et ceci quelle qu'en soit l'origine réelle.

Elle relève que dès la réalisation du contrôle du 19 février 2014, la société s'est montrée diligente pour limiter l'effet du défaut de sécurisation de l'application. Cependant sans qu'il soit nécessaire de se prononcer sur la date de la connaissance avérée de la faille dont il est discuté, la formation restreinte ne peut que constater qu'éclairée sur l'existence d'une faille de sécurité interne, la société n'a entrepris aucune démarche pour vérifier la sécurité de l'ensemble de l'application. Elle est ainsi restée dans l'ignorance de la seconde faille de sécurité, révélée lors du contrôle, alors que cette faille présente nécessairement par sa nature des conséquences plus importantes à l'égard des personnes.

Si l'obligation de sécurisation prévue par l'article 34 de la loi du 6 janvier 1978 modifiée n'impose pas une obligation de résultat au responsable de traitement, celui-ci ne peut trouver à s'exonérer de sa responsabilité quant à l'existence d'un défaut de sécurité dont il apparaît qu'il

existe depuis un temps indéterminé et qui n'a été mis en évidence que par l'action de la CNIL alors que la société déclarait connaître un autre défaut de sécurité affectant la même application.

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

2. **Sur le manquement à l'obligation de définir une durée de conservation**

L'article 6-5° de la loi du 6 janvier 1978 modifiée dispose qu'un traitement ne peut porter que sur des données à caractère personnel qui *« sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »*

Il est établi par procès-verbal que la plus ancienne des fiches clients présente dans l'application « avis de passage » est datée de l'année 2007. Une durée de conservation des données des clients pour une période aussi longue doit être justifiée et ne pas excéder les nécessités de la réalisation du traitement.

En défense la société fait valoir qu'elle a procédé en février 2014 à une purge des données et à la mise en place d'une politique de limitation de la durée de conservation des données proportionnée à la réalisation de la finalité du traitement. Cette durée est fixée à un mois glissant à compter de la migration vers la nouvelle application au mois de mars 2014.

La formation restreinte prend acte de ces éléments pour l'avenir mais constate que la société ne justifie pas antérieurement à cela d'une politique limitant la durée de conservation des données.

Il en résulte nécessairement, en l'absence de justification, que la durée de conservation observée excède manifestement les besoins de la relation client dont l'objet est principalement d'assurer la livraison rapide de biens au domicile des personnes.

La formation restreinte considère que la société n'a pas respecté les dispositions de l'article 6-5° de la loi du 6 janvier 1978 modifiée.

Sur la sanction et la publicité

La formation restreinte retient que la société n'a pas respecté les dispositions prévues aux articles 34 et 6-5° de la loi n°78-17 du 6 janvier 1978 modifiée.

Par conséquent, la formation restreinte décide de prononcer à son encontre la sanction de l'avertissement prévu à l'article 45 de la loi n°78-17 du 6 janvier 1978 modifiée.

Au regard du nombre de personnes concernées, de la nature des données accessibles sans restriction, la formation restreinte décide de rendre cette décision publique sans assurer l'anonymisation du nom commercial de la société demandée par cette dernière au cours de la séance.

PAR CES MOTIFS

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

De prononcer un avertissement à l'encontre de la société DHL International Express France

De rendre publique sa décision sur le site Internet de la CNIL et sur le site Légifrance.

Le Président

Jean-François CARREZ

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'Etat dans un délai de deux mois à compter de sa notification.