Commission Nationale de l'Informatique et des Libertés

Délibération n°2016-265 du 20 septembre 2016

Délibération de la formation restreinte n° 2016-265 du 20 septembre 2016 prononçant un avertissement public à l'encontre de la société CDISCOUNT

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, 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 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° 2016-011C du 4 février 2016 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 auprès de la société CDISCOUNT ;

Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur, en date du 2 mai 2016 ;

Vu le procès-verbal de contrôle sur place n° 2016-011/1 du 11 février 2016 ;

Vu le rapport de M. Éric PERES, commissaire rapporteur, notifié à la société CDISCOUNT le 20 mai 2016 ;

Vu la demande de huis clos présentée par la société CDISCOUNT le 16 juin 2016 à laquelle il a été fait droit par courrier du 28 juin 2016 ;

Vu les observations écrites de la société CDISCOUNT reçues le 23 juin 2016, 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 30 juin 2016,

- M. Éric PERES, commissaire, en son rapport ;

- M. Jean-Alexandre SILVY, Commissaire du Gouvernement, n'ayant pas formulé d'observation ;

- Madame X de la société CDISCOUNT ;

- Monsieur Y de la société CDISCOUNT ;

- Maitre Z, Avocat du cabinet Z.

La représentante de la société CDISCOUNT ayant pris la parole en dernier ;

A adopté la décision suivante :

I. Faits et procédure

La société CDISCOUNT (ci-après la société ou la société CDISCOUNT) a pour activité principale la vente de produits aux particuliers sur Internet. Son site internet www.cdiscount.com indique compter environ 2 millions de visiteurs et 85.000 ventes par jour. La société exerce également une activité de vente à distance par téléphone.

La CNIL a reçu 80 plaintes depuis 2015 concernant la société CDISCOUNT relatives notamment à des défaillances techniques qui auraient entraîné la divulgation de données à caractère personnel à des tiers non autorisés.

En application de la décision n° 2016-011C du 4 février 2016 de la Présidente de la CNIL, plusieurs contrôles en ligne et sur place ont été réalisés entre février et mars 2016 afin de vérifier le respect par la société des dispositions de la loi du 6 janvier 1978 modifiée. Dans ce cadre, une délégation de la Commission a procédé à une mission de contrôle dans les locaux de la société CDISCOUNT le 11 février 2016.

A cette occasion, la délégation de contrôle a constaté que la société CDISCOUNT conservait 4179 numéros de cartes bancaires de clients en clair dans les champs commentaires de sa base de données. Elle a également constaté la présence dans ces mêmes champs, de plus de 3000 cryptogrammes visuels associés aux numéros des cartes bancaires des clients dont certaines encore valides.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. Éric PERES en qualité de rapporteur, le 2 mai 2016, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée.

A l'issue de son instruction, le rapporteur a notifié à la société le 20 mai 2016 par huissier, un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la CNIL de prononcer 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 30 juin 2016 indiquant à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites.

La société CDISCOUNT a produit le 23 juin 2016 des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 30 juin 2016.

II. Motifs de la décision

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 CDISCOUNT a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données des personnes concernées par le traitement et notamment des mesures adaptées pour que ces données ne soient pas accessibles à des tiers non autorisés.

Le contrôle sur place du 11 février 2016 a permis de constater que la société conservait en clair dans les champs de commentaires de sa base de données, 4179 numéros de cartes bancaires de clients. Parmi ces numéros, figuraient 2104 cartes bancaires valides au jour du contrôle auxquelles était associé un cryptogramme.

A la suite du contrôle, la délégation a en outre été informée, notamment par la fourniture du registre du Correspondant Informatique et Libertés, que ces données étaient accessibles par les prestataires auxquels faisait appel la société.

En défense, la société indique qu'une équipe interne [...] est dédiée aux aspects relatifs à la sécurité des systèmes d'information et que l'accès aux données à caractère personnel traitées fait l'objet d'un contrôle strict.

Elle fait également valoir que les numéros de cartes bancaires ainsi que les cryptogrammes associés, présents dans les champs de commentaires, ont été collectés dans le cadre d'une activité accessoire de la société, celle de la vente à distance par téléphone, la vente en ligne sur internet représentant son activité principale.

La société estime par ailleurs que les faits révèlent une dérive opérationnelle plutôt qu'une faille de sécurité. Elle indique notamment que le manquement reproché trouve son origine dans l'erreur commise par l'un de ses prestataires [...] et le non-respect des instructions données, les informations bancaires n'ayant pas à être enregistrées dans les champs de commentaires de la base de données.

Enfin, la société fait valoir les actions correctives mises en place. Elle indique notamment avoir procédé à la purge des données bancaires, résilié le contrat avec le prestataire en cause, adressé des lettres de mise en demeure aux autres prestataires et mis en place un contrôle automatisé des champs de commentaires.

La formation restreinte prend acte des mesures correctives prises a posteriori par la société mais considère que cette dernière, bien que s'étant dotée d'un Correspondant Informatique et Libertés depuis 2009 ainsi que d'une équipe technique dédiée, n'a pas mis en œuvre de moyens suffisants pour répondre à l'obligation de sécurité et de confidentialité des données imposée par la loi du 6 janvier 1978 modifiée.

En effet, la société a conservé en clair 4179 numéros de cartes bancaires de clients dans des champs de commentaires dont ce n'est pas l'objet et qui sont dépourvus de mesures de sécurité particulières d'obfuscation ou tokenisation permettant de garantir la sécurité des données et d'empêcher que des tiers non autorisés y aient accès.

Au surplus, l'accessibilité par l'ensemble des prestataires externes à la société aux données bancaires en clair des clients était susceptible d'entraîner une utilisation frauduleuse de ces données.

Par ailleurs, si les faits constatés ne portent que sur l'activité de vente par téléphone de la société, la formation restreinte estime que la circonstance selon laquelle l'origine du manquement résulterait du non-respect de ses instructions par un prestataire n'est pas de nature à amoindrir la gravité du manquement et de ses effets, et ne saurait en aucune façon exonérer l'organisme de sa responsabilité et de ses obligations.

En effet, la formation restreinte rappelle que conformément à l'article 35 alinéa 3 de la loi du 6 janvier 1978 modifiée, le recours à un sous-traitant ne décharge pas le responsable de traitement de son obligation de veiller au respect des mesures de sécurité et de confidentialité.

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.

2. Sur le manquement à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement

L'article 6-5 de la loi du 6 janvier 1978 modifiée dispose que les données à caractère personnel 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 .

La norme simplifiée n° 48 relative à la gestion des clients et des prospects, en référence de laquelle la société a pris plusieurs engagements de conformité, prévoit notamment que les données à caractère personnel relatives aux clients ne peuvent être conservées au-delà de la durée strictement nécessaire à la gestion de la relation commerciale. [...] Par ailleurs, et sous réserve du respect de l'article 6 de la présente norme, les données des clients utilisées à des fins de prospection commerciale peuvent être conservées pendant une durée de trois ans à compter de la fin de la relation commerciale (c'est-à-dire par exemple à compter d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestation de services, du dernier contact émanant du client) .

Les données à caractère personnel relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (demande de documentation, par exemple). Au terme de ce délai de trois ans, le responsable de traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées conformément aux dispositions en vigueur, et notamment celles prévues par le code de commerce, le code civil et le code de la consommation .

Il appartient à la formation restreinte de décider si la société a manqué à l'obligation lui incombant, en application de ces dispositions, s'agissant de deux catégories de données : les cryptogrammes visuels correspondant aux cartes bancaires enregistrées et les comptes en ligne des clients et des prospects de la société.

- Sur la conservation des cryptogrammes visuels des cartes bancaires

Le contrôle du 11 février 2016 a permis de constater que parmi les 4179 numéros de cartes bancaires, figuraient en clair dans la base de données de la société, plus de 3000 numéros de cartes bancaires associées à des cryptogrammes dont 2104 numéros de cartes bancaires encore valides.

En défense, la société fait valoir que ces données n'ayant pas vocation à être enregistrées dans les champs commentaires de la base de données, aucune durée de conservation n'a été définie les concernant.

La formation restreinte considère que si la société a rapidement procédé à la purge de ces données à l'issue du contrôle de la CNIL, elle a néanmoins conservé les cryptogrammes visuels des cartes bancaires de ses clients pendant une durée excessive.

En effet, l'unique finalité du cryptogramme visuel est de s'assurer que le client est bien en possession physique de la carte bancaire utilisée. En conséquence, une fois cette vérification ponctuelle effectuée, sa conservation est interdite au-delà du temps strictement nécessaire à la réalisation de la transaction bancaire, y compris en cas de paiements successifs ou de conservation du numéro de la carte pour des achats ultérieurs.

La formation restreinte considère également que la conservation d'un nombre important de cryptogrammes associés à des cartes encore valides représente un risque supplémentaire pour les personnes.

- Sur la conservation des données des comptes clients et des prospects

Le contrôle a permis de constater que la base active de la société contenait [...] de comptes relatifs à des clients ou prospects. Parmi eux, [...] de comptes correspondaient à des clients n'ayant pas validé de commande depuis plus de trois ans et [...] de comptes étaient relatifs à des prospects (n'ayant jamais validé de commande) ayant créé un compte depuis plus de trois ans.

En défense, si la société ne conteste pas ces éléments, elle indique qu'un projet de définition d'une durée d'archivage et de purge de la base de données est prévu pour 2016. Elle précise que ce projet fixe de nouvelles durées de conservation des comptes clients et prospects en base active et en archive intermédiaire ainsi que la date à compter de laquelle ces données seront anonymisées ou purgées.

Si la formation restreinte prend acte des travaux en cours de la société sur la durée de conservation de ces données, elle considère néanmoins que la société n'a pas pris les mesures nécessaires pour se conformer à ses propres engagements de conformité à la norme simplifiée n°48. En l'espèce, la société n'a défini aucune règle de conservation, ni mis en œuvre de mécanisme d'archivage ou de purge des données des clients et des prospects.

Elle estime par ailleurs que les instructions adressées au service informatique de la société ne résultent que de l'engagement d'une procédure de sanction.

La formation restreinte considère que le manquement aux obligations découlant de l'article 6-5° de la loi du 6 janvier 1978 modifiée est caractérisé.

3. Sur la sanction et la publicité

Les manquements commis par la société CDISCOUNT justifient que soit prononcé à son encontre un avertissement.

Compte tenu de la nature et du nombre de données en cause, à savoir 4179 numéros de cartes bancaires associés pour une partie d'entre eux aux cryptogrammes visuels, ainsi que de la nécessité de sensibiliser le secteur marchand de la vente à distance et les responsables de

traitements quant à leurs obligations en la matière, la formation restreinte décide de rendre publique sa décision.

PAR CES MOTIFS

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

- de prononcer un avertissement à l'encontre de la société CDISCOUNT ;

- de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

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.