

La Présidente de la Commission nationale de l'informatique et des libertés ;

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code pénal ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 45 ;

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 les décisions n° 2015-044C du 4 février 2015 et n° 2015-193C du 22 avril 2015 de la Présidente de la Commission nationale de l'informatique et des libertés de procéder à des missions de vérification auprès de la société BOULANGER et de tous les traitements de données à caractère personnel relatif au site internet BOULANGER.COM ;

Vu le procès-verbal de contrôle sur place n° 2015-044 du 10 février 2015, ainsi que le procès-verbal de constatations en ligne n° 2015-193 du 23 avril 2015 ;

Vu la plainte n° [REDACTED] ;

I- Constate les faits suivants

La société BOULANGER (ci-après « la société »), sise rue de la Haie Plouvier à Fretin (59273), gère des magasins physiques, ainsi qu'un site internet, spécialisés dans le multimédia et l'électroménager. Elle emploie environ 8000 personnes.

En application des décisions n° 2015-044C et n° 2015-193C des 4 février 2015 et 22 avril 2015 de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après

Commission Nationale de l'Informatique et des Libertés

« la CNIL » ou « la Commission »), une délégation de la CNIL a procédé, le 10 février 2015, à une mission de contrôle auprès du magasin BOULANGER situé 53, route de Thonon à ANNEMASSE (74100), ainsi qu'à des constatations en ligne le 23 avril 2015 sur le site BOULANGER.COM (ci-après « le site internet »). La délégation s'est attachée à examiner la conformité des traitements de données à caractère personnel mis en œuvre par la société, ou pour son compte, aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée, et en particulier d'instruire la plainte n° [REDACTED].

La société met à disposition de l'ensemble de ses magasins un outil leur permettant notamment de gérer les clients pour lesquels une facture est éditée. Cet outil permet aux salariés des magasins de mettre à jour les fiches clients et d'ajouter des commentaires.

A cet égard, la délégation a constaté la présence de commentaires non pertinents concernant les clients de la société.

Elle a également constaté, sur le site internet de la société, le dépôt de cookies à finalité publicitaire dès l'arrivée sur la page d'accueil, ainsi que la conservation des données enregistrées dans certains de ces cookies pendant des durées pouvant aller jusqu'à 15 ans.

II- Sur les manquements constatés au regard des dispositions de la loi du 6 janvier 1978 modifiée

Un manquement à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données

La délégation a été informée que la société met à disposition de ses magasins un outil national de gestion des clients pour lesquels une facture a été éditée. Le service après vente (ci-après « le SAV ») utilise le menu « intervention » de cet outil pour gérer les réparations.

A cet égard, la délégation a constaté, dans le menu « intervention » la présence de 5 828 commentaires non pertinents, comme par exemple « CLIENT TRES AGRESSIF », « N'A PAS DE CERVEAU », « LE CLIENT EST CHIANT », « CLIENT TRES CON », « LA CLIENTE EST UNE GROSSE CONNASSE QUI SE CROIT TOUT PERMIS », « CLIENT CASSE COUILLE », « FOLLE », « FORT ACCENT AFRICAIN », « CLIENTE DE CONFESSION JUIVE », « CLIENTE AVEC PROBLEME CARDIAQUE », « CLIENTE A UNE MALADIE NEUROLOGIQUE », « CLIENT ALCOOLIQUE », « ME PASSE SON

MARI ATTEINT DE PARKINSON », « CLIENT C'EST FAIT OPERE DUNE HERNIE DISCAL IL Y A 3 MOIS ».

Ces faits constituent un manquement aux obligations prévues au 3° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée, qui dispose que les données à caractère personnel collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Un manquement à l'obligation d'informer et d'obtenir l'accord préalable des personnes concernées avant d'inscrire des informations (cookies) sur leur équipement terminal de communications électroniques ou d'accéder à celles-ci (lecture des cookies)

A titre liminaire, la Commission rappelle que l'article 32-II de la loi du 6 janvier 1978 modifiée dispose que *« Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :*

- *de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement;*
- *des moyens dont il dispose pour s'y opposer.*

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- *soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;*
- *soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ».*

Afin de proposer aux professionnels du secteur des lignes directrices en la matière, la CNIL a adopté la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs. Cette recommandation, qui n'a pas de valeur impérative, vise à interpréter les dispositions législatives précitées et à éclairer les acteurs sur la mise en place de mesures concrètes permettant de garantir le respect de ces dispositions, afin, soit qu'ils mettent en œuvre ces mesures, soit qu'ils mettent en œuvre des mesures d'effet équivalent.

Les cookies nécessitant une information et un consentement préalables de l'internaute sont notamment les cookies liés aux opérations relatives à la publicité ciblée et les cookies traceurs de réseaux sociaux générés par les « boutons de partage de réseaux sociaux ».

La recommandation de la CNIL rappelle que « *la validité du consentement est liée à la qualité de l'information reçue* ». La Commission recommande donc que ce consentement soit recueilli en deux étapes :

- première étape : « *l'internaute qui se rend sur le site d'un éditeur (page d'accueil ou page secondaire du site) doit être informé, par l'apparition d'un bandeau : des finalités précises des Cookies utilisés ; de la possibilité de s'opposer à ces Cookies et de changer les paramètres en cliquant sur un lien présent dans le bandeau ; du fait que la poursuite de sa navigation vaut accord au dépôt de Cookies sur son terminal* » ;
- seconde étape : « *les personnes doivent être informées de manière simple et intelligible des solutions mises à leur disposition pour accepter ou refuser tout ou partie des Cookies nécessitant un recueil du consentement : pour l'ensemble des technologies visées par l'article 32-II précité ; par catégories de finalités : notamment la publicité, les boutons des réseaux sociaux et la mesure d'audience* ».

En outre, la recommandation indique que l'information « *doit être visible, mise en évidence et complète* ».

En l'espèce, lorsque la délégation s'est connectée au site internet de la société, elle a constaté que 108 cookies ont été déposés sur son équipement terminal. Par courrier électronique reçu par la CNIL le 6 mai 2015, la société a indiqué que 90 de ces cookies ont une finalité publicitaire.

La délégation a constaté que les internautes sont informés du dépôt des cookies par un bandeau précisant ce qui suit : « *En poursuivant votre navigation, vous acceptez l'utilisation des cookies pour disposer de contenus adaptés à vos centres d'intérêt et améliorer votre expérience sur le site. Pour en savoir plus et gérer vos paramètres, [cliquez ici](#)* ».

En outre, la délégation a constaté que le lien hypertexte « *cliquez ici* » présent sur ce bandeau renvoie vers la rubrique « *Utilisation des cookies* » de la page intitulée « *Mentions légales* », qui informe les internautes de la possibilité qui leur est offerte de refuser les cookies en paramétrant leur navigateur. Ce paramétrage est, en l'espèce, un moyen valable d'opposition dans la mesure où le site ne dépose pas de cookies techniques essentiels à son fonctionnement (qui seraient bloqués si l'internaute décidait de bloquer tous les cookies à partir de son navigateur, ce qui l'empêcherait d'utiliser le site).

Mais la délégation a constaté que le dépôt de cookies dans l'équipement terminal de communications électroniques de l'internaute s'opère dès la connexion au site internet, avant toute action de la part de l'internaute tendant à poursuivre sa navigation sur le site.

Au regard de ce qui précède, il apparaît que le site internet n'a pas recueilli le consentement des personnes concernées avant de procéder au dépôt des cookies.

L'ensemble de ces faits constitue un manquement au II de l'article 32 précité de la loi du 6 janvier 1978 modifiée, qui soumet notamment à information et à accord préalables de l'internaute le dépôt de tels cookies.

En outre, il est rappelé qu'en application des articles 131-41 et R. 625-10 du code pénal combinés, le fait pour la personne morale responsable d'un traitement de ne pas informer les personnes concernées et obtenir leur accord avant d'accéder à ou d'inscrire des informations dans leur équipement terminal de communications électroniques est puni d'une peine d'amende pouvant atteindre 7.500 €.

Un manquement à l'obligation de définir et respecter une durée de conservation des données proportionnée à la finalité du traitement

La délégation a constaté que les données enregistrées dans certains cookies déposés par le site internet de la société sont accessibles pendant une durée excessive par rapport aux finalités poursuivies. En effet, elle a constaté que certains cookies à finalité publicitaire ont une durée de vie pouvant aller jusqu'à 15 ans.

A cet égard, la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs précise que *« les Cookies doivent (...) avoir une durée de vie limitée à treize mois après leur premier dépôt dans l'équipement terminal de l'utilisateur (faisant suite à l'expression du consentement) et leur durée de vie ne doit pas être prolongée lors de nouvelles visites sur le site »*.

L'ensemble de ces faits constitue un manquement aux obligations découlant du 5° de l'article 6 de la loi du 6 janvier 1978 modifiée qui 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.

Il est en outre rappelé qu'en application des articles 226-24 et 226-20 du code pénal combinés, le fait pour une personne morale, de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni d'une peine d'amende pouvant atteindre 1.500.000 €.

Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données

[REDACTED]

[REDACTED]

[REDACTED]

Ces faits constituent un manquement à l'article 34 de la loi n° 78-17 du 6 janvier 1978 disposant 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 est en outre rappelé qu'en application des articles 226-24 et 226-17 du code pénal combinés, le fait pour une personne morale de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni d'une peine d'amende pouvant atteindre 1.500.000 €.

En conséquence, la société BOULANGER, sise rue de la Haie Plouvier à Fretin (59273)), est mise en demeure, sous un délai de trois (3) mois à compter de la notification de la présente décision, pour l'ensemble de ses magasins et sites internet, et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

- **prendre les mesures nécessaires pour éviter que des commentaires excessifs ne soient enregistrés dans les bases de données de la société, et en particulier mettre en place un système de détection automatique de ces derniers et attirer l'attention des salariés sur la nécessité de n'enregistrer que des données adéquates et pertinentes ;**
- **obtenir l'accord préalable des personnes concernées à l'inscription d'informations sur leur équipement terminal (cookies) et à l'accès à celles-ci (lecture des cookies). A cet égard, il appartient à la société de conditionner cette inscription et cet accès à une action positive préalable des personnes concernées ;**
- **ne pas déposer de cookies dont la durée de validité est supérieure à treize mois après leur dépôt sur l'équipement terminal de la personne concernée ;**
- **prendre toute mesure de sécurité, pour l'ensemble des traitements de données à caractère personnel qu'elle met en œuvre, permettant de préserver la sécurité des données et d'empêcher que des tiers non autorisés y aient accès, notamment :**

- [REDACTED]
- **justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.**

À l'issue de ce délai, si la société BOULANGER s'est conformée à la présente mise en demeure, il sera considéré que la procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, s'il est constaté que la société BOULANGER ne s'est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de la Commission de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente



Isabelle FALQUE-PIERROTIN