**Délibération de la CNIL n° 2008-118 du 20 mai 2008 prononçant un avertissement à l'encontre de la société ENTREPARTICULIERS.CO**

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TURK ;
Etant aussi présents, M. Guy ROSIER, vice-président délégué, M. François GIQUEL, vice-président, Mlle Anne DEBET, membre, M. Bernard PEYRAT, membre et M. Hubert BOUCHET, membre ;
Vula 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° 2004-801 du 6 août 2004 ;
Vule 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° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;
Vu la délibération n° 2007-311 du 25 octobre 2007 de la Commission nationale de l'informatique et des libertés mettant en demeure la société ENTREPARTICULIERS.COM, notifiée le 14 décembre 2007 ;
Vula décision n° 2008-045C du 27 mars 2008 du président de la Commission nationale de l'informatique et des libertés de procéder à une mission de vérification auprès de la société ENTREPARTICULIERS.COM ;
Vules plaintes n° 06011355, 08001998 et 08006799 ;
Vu le rapport de M. Jean MASSOT, commissaire rapporteur, notifié par porteur à la société ENTREPARTICULIERS.COM le 18 avril 2008 ;
Vu les autres pièces du dossier ;
Après avoir entendu, lors de la réunion du 20 mai 2008 :

- M. Jean MASSOT, commissaire, en son rapport ;
- Mme Pascale COMPAGNIE, commissaire du Gouvernement, en ses observations ;
- Maître Corinne LE FLOCH, avocat de la société ENTREPARTICULIERS.COM ;

Maître Corinne LE FLOCH ayant pris la parole en dernier ;

1. Faits et procédure
2. Faits

1. La société ENTREPARTICULIERS.COM dispose d'un site internet dénommé « entreparticuliers.com », qui a pour but de faciliter la mise en relation de vendeurs et d'acheteurs particuliers de biens immobiliers. Ce traitement a fait l'objet d'une déclaration de site internet auprès de la Commission nationale de l'informatique et des libertés (ci-après « CNIL » ou « Commission »), le 22 décembre 2005.
2. La CNIL a été saisie, le 7 juillet 2006, d'une plainte de M. G qui, à la suite de sa demande de diffusion d'une annonce relative à la vente de son appartement sur le site internet « entreparticuliers.com », s'est vu sollicité à plusieurs reprises par des agences immobilières, alors même que son annonce n'avait pas encore été diffusée sur ledit site et qu'elle précisait « agences s'abstenir ».
M. G a également été contacté par un particulier, qui s'est ensuite présenté à un rendez-vous fixé par le plaignant, accompagné d'un représentant de l'agence GUERNIER (ORPI Rouen).

Ce représentant a informé M. G qu'il disposait des annonces communiquées par la société ENTREPARTICULIERS.COM ainsi que des coordonnées des personnes en ayant demandé la diffusion.
Les services de la Commission ont demandé à la société ENTREPARTICULIERS.COM, par un courrier du 31 juillet 2006, de bien vouloir lui faire part de ses observations sur la sollicitation de M. G par des agences immobilières, alors même que l'annonce dont il a demandé la diffusion n'était pas encore parue. En l'absence de réponse de la société ENTREPARTICULIERS.COM, la Commission a adressé un courrier de relance le 26 septembre 2006.
Le 10 novembre 2006, la société ENTREPARTICULIERS.COM a adressé une réponse dans laquelle elle demandait de lui « faire parvenir des éléments tangibles qui permettent au dénommé G d'affirmer qu'à la suite de sa demande de diffusion d'une annonce relative à la vente de son appartement sur le site « entreparticuliers.com », il s'est vu sollicité à plusieurs reprises par d'autres agences immobilières alors même que son annonce n'avait pas été diffusée ».
Par un courrier du 19 avril 2007, la Commission a de nouveau sollicité les observations de la société ENTREPARTICULIERS.COM et lui a demandé de préciser, dans un délai de quinze jours, si elle avait « communiqué les coordonnées du requérant à des sociétés tierces » et, dans cette hypothèse, « comment les personnes ont été informées de leurs droits et de la possibilité qui leur est offerte de s'opposer à la transmission de leurs coordonnées à des tiers comme le prévoit la loi informatique et libertés ».
Ce courrier est resté sans réponse.

1. Procédure

3. En conséquence, par délibération n° 2007-311 du 25 octobre 2007, la formation restreinte de la Commission a mis en demeure la société ENTREPARTICULIERS.COM, sise 105 rue Jules Guesde à Levallois-Perret (92300), sous un délai de quinze jours à compter de la notification de la décision (le 14 décembre 2007) de :

- informer la Commission sur les raisons pour lesquelles les coordonnées de M.G, ainsi que l'annonce dont il a souhaité la diffusion sur le site internet « entreparticuliers.com », auraient été communiquées à des tiers ;
- communiquer à la CNIL l'intégralité des procédures mises en œuvre visant à informer et à permettre aux clients d'exercer les droits offerts par les dispositions des articles 32 (droit à l'information) 38 (droit d'opposition), 39 et 40 (droit de rectification) de la loi du 6 janvier 1978 ;
- préciser les mesures de sécurité prises (sensibilisation du personnel, politique de sécurité, contrôles réguliers du contenu des fichiers, etc.) pour assurer la sécurité des traitements de données à caractère personnel mis en œuvre par la société ENTREPARTICULIERS.COM.

4. En réponse à la mise en demeure, la société ENTREPARTICULIERS.COM a adressé à la CNIL deux courriers, en date des 21 décembre 2007 et 29 janvier 2008, dans lesquels elle a affirmé ne transférer aucune donnée figurant dans ses fichiers à des tiers. Elle a également signifié l'existence de sociétés qui capturent en temps réel les annonces immobilières publiées sur son site internet.
5. Le 23 janvier 2008, la Commission a été saisie d'une plainte de M. H à l'encontre de la société ENTREPARTICULIERS.COM, relative à des failles de sécurité du site internet. Le plaignant indiquait en effet qu'il était possible d'accéder aux informations personnelles

d'autres annonceurs en tapant son code personnel, attribué lors de la mise en ligne de sa propre annonce.
Par ailleurs, M. S, ayant des difficultés à faire exercer son droit de suppression de ses coordonnées bancaires par la société ENTREPARTICULIERS.COM, s'est également rapproché de la CNIL, le 14 mars 2008. Cette société n'a, en effet, apporté aucune réponse aux demandes successives du plaignant adressées par courriers en date des 21 novembre 2007 et 9 janvier 2008.
6.En application de la décision n° 2008-045C du 27 mars 2008 du président de la CNIL, une délégation de la Commission a procédé à une mission de vérification sur place le 31 mars 2008, afin d'apprécier les conditions de mise en œuvre du site internet « entreparticuliers.com », au regard des dispositions de la loi du 6 janvier 1978 modifiée et des différentes plaintes dont la CNIL a été saisie.
La délégation de la Commission a tout d'abord constaté qu'un particulier, souhaitant mettre en ligne une annonce sur le site internet « entreparticuliers.com », doit saisir préalablement un ensemble d'informations personnelles, notamment ses nom et prénom, son numéro de téléphone, son adresse électronique et ses coordonnées bancaires s'il décide de payer en ligne. D'autres choix sont possibles quant au mode de paiement. L'annonceur peut en effet demander que le service clientèle de la société le rappelle afin qu'il communique personnellement à son interlocuteur les informations bancaires nécessaires ou peut également choisir de régler par chèque.
Les informations sont ensuite stockées dans une base de données de type « Access » pour la gestion et la facturation des annonces. Les données bancaires saisies n'y restent environ qu'une heure, et sont extraites de manière automatique pour être enregistrées dans une autre base de données de type « SQL ». La délégation a cependant constaté que de nombreux fichiers intermédiaires ou de sauvegarde ainsi que des tables de traitement, utilisées, à titre d'exemple, pour le prélèvement ou la gestion du centre d'appels, contiennent des informations bancaires qui auraient dû être effacées.
La délégation de la Commission a ensuite relevé qu'aucune politique de conservation de l'ensemble des données n'a été définie. En outre, le réseau interne de la société ENTREPARTICULIERS.COM n'était pas cloisonné et des dysfonctionnements ont en effet été constatés s'agissant de l'effacement des informations bancaires.
La mission de contrôle a par ailleurs permis de constater une absence de cloisonnement du réseau interne de la société ENTREPARTICULIERS.COM. En effet, si les postes informatiques de la majorité des employés ne permettaient pas la lecture des données figurant dans les fichiers de gestion et de facturation des annonces, car ils n'étaient pas configurés pour accéder à des bases de données de type « Access », ces données (en particulier les coordonnées bancaires) pouvaient cependant être copiées sur un support informatique amovible et alors être lues à partir d'un poste informatique sur lequel aurait été installé le logiciel « Access ». Dès lors, les salariés pouvaient prendre connaissance des informations à caractère personnel, relatives aux annonceurs, alors même qu'ils n'étaient pas autorisés à y avoir accès.
La délégation de la CNIL a également relevé qu'il était possible d'accéder aux annonces immobilières mises en ligne sur le site internet « entreparticuliers.com » et de les modifier ou de les supprimer, ainsi que d'accéder à la facture de l'annonce. A cette fin, il suffisait d'inscrire, dans la partie « gérer votre annonce» du site internet, la référence d'une annonce puis de saisir, dans la partie « nom associé à votre référence », le nom de n'importe quel client. De fait, un simple nom générique tel que « Dupont » ou « Durant » (de nombreux clients portent ces patronymes) ou le nom d'un autre annonceur permettait d'accéder aux espaces personnels de tous les annonceurs. En changeant le numéro de l'annonce mais en utilisant à chaque fois le même nom d'un client, on accédait aux éléments indiqués ci-dessus,

normalement réservés au seul annonceur. Il a été reconnu par le personnel de la société qu'une erreur de programmation sur le contrôle d'accès par les clients à leur espace personnel était à l'origine de cette faille de sécurité.
La société ENTREPARTICULIERS.COM a déclaré acheter des fichiers d'annonces immobilières, captées à partir d'autres sites internet concurrents, contenant des coordonnées d'annonceurs, à qui elle envoie ses campagnes de prospection commerciale par sms ou par courrier électronique. Le consentement préalable des personnes ainsi sollicitées n'était pas recueilli.
S'agissant du droit de suppression, la délégation de la Commission a constaté que les coordonnées bancaires de M. S, qui en avait demandé la suppression, figuraient toujours dans certaines bases de données de la société ENTREPARTICULIERS.COM.
Enfin, la délégation de la CNIL a relevé que la société ENTREPARTICULIERS.COM a introduit sur son site internet une case « Vie Privée » pour informer les internautes des droits d'accès, de modification et de suppression des données à caractère personnel dont ils disposent, mais qui faisait référence à un mauvais article de la loi « Informatique et Libertés ».
7. Sur la base des constatations opérées par la délégation de la CNIL lors de cette mission de contrôle, une proposition d'avertissement a été notifiée par porteur à la société ENTREPARTICULIERS.COM, le 18 avril 2008, à laquelle était jointe la convocation à l'audience du 20 mai 2008. Le rapport de sanction faisait état des différents manquements constatés à la loi « informatique et libertés », à savoir ceux relatifs à l'obligation de sécurité et de confidentialité des données traitées, à l'obligation de définition de leurs durées de conservation, à l'obligation de consentement préalable des personnes, au droit d'information des personnes et au droit de suppression des données.

1. Motifs de la décision :
2. Lors de l'audience de sanction du 20 mai 2008, la société ENTREPARTICULIERS.COM a présenté à la formation restreinte de la CNIL les différentes mesures prises afin de se mettre en conformité avec la loi du 6 janvier 1978 modifiée et a précisé avoir effectué une déclaration simplifiée selon la norme simplifiée n° 48 pour la gestion de ses clients et prospects.

A) Sur l'obligation de sécurité et de confidentialité des données à caractère personnel
9. Le rapporteur a considéré que la société ENTREPARTICULIERS.COM n'avait pas respecté les dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée, au vu des failles de sécurité constatées lors de la mission de contrôle de la CNIL. En effet, le réseau interne de la société ENTREPARTICULIERS.COM n'était pas cloisonné et une faille de sécurité sur le portail du site internet « entreparticuliers.com » a été constatée, rendant possible un accès à tous les espaces personnels des annonceurs (permettant notamment de modifier ou supprimer les annonces ou d'accéder aux factures), en inscrivant dans la partie « gérer votre annonce» du site internet la référence d'une annonce, puis en saisissant dans la partie « nom associé à votre référence » le nom de n'importe quel client.
La société ENTREPARTICULIERS.COM a apporté à la formation restreinte de la CNIL, lors de l'audience du 20 mai 2008, les extractions de certains fichiers intermédiaires et de sauvegarde sur lesquelles ne figurent plus les coordonnées bancaires des clients. La société a également indiqué avoir mis en place trois bases de données, qui font désormais l'objet de purges automatiques à des étapes différentes, la dernière intervenant une fois la transaction terminée sur la base de données définitive. Elle a souligné la mise en place d'un paiement sécurisé avec la BANQUE POSTALE, qui sera effectif à compter du mois de juin 2008.
La société ENTREPARTICULIERS.COM a également indiqué avoir corrigé les failles de sécurité du site internet et a apporté certaines garanties quant à la confidentialité des données

transmises par les annonceurs et au fait qu'elles ne puissent pas être consultées par des tiers non-autorisés.
La société ENTREPARTICULIERS.COM a informé la formation restreinte de la CNIL de la mise en place d'un serveur d'authentification pour gérer les accès aux données. Les salariés font en outre l'objet d'une politique de traçabilité permettant à la société de savoir ce que les employés consultent dans les bases de données.
Aucune donnée technique n'a été communiquée à la CNIL par la société ENTREPARTICULIERS.COM concernant les accès et les profils d'accès aux données à caractère personnel traitées et aucune information précise n'a été apportée s'agissant de la politique de gestion des mots de passe. Aucune information n'a été, en outre, apportée sur les modalités techniques d'effacement des données des clients ayant souhaité que celles-ci soient supprimées.

1. Sur la durée de conservation des données

10. Il ressort également des conclusions du rapporteur qu'aucune durée de conservation des données à caractère personnel traitées par la société ENTREPARTICULIERS.COM n'était définie, contrairement aux dispositions du 5° de l'article 6 de la loi du 6 janvier 1978 modifiée.
La société ENTREPARTCULIERS.COM a indiqué, lors de l'audience du 20 mai 2008, que les données relatives aux annonceurs sont effacées dans les conditions prévues par la norme simplifiée n° 48 de la CNIL qui prévoit que les données ne peuvent être conservées au-delà de la relation commerciale sauf celles nécessaires pour établir la preuve d'un droit ou d'un contrat qui peuvent être archivées dix ans.

1. Sur l'obligation de consentement préalable

11. Le rapport proposant de prononcer un avertissement à l'encontre de la société ENTREPARTICULIERS.COM précisait que la délégation de la CNIL avait constaté que cette société achetait des fichiers d'annonces immobilières, qui contenaient notamment les coordonnées de différents annonceurs. La société ENTREPARTICULIERS.COM constituait ensuite de nouveaux fichiers avec les numéros de téléphone et les adresses électroniques, afin de démarcher les personnes dans le cadre de ses campagnes de prospection commerciale par sms ou par courrier électronique.
Le rapporteur avait souligné que la société ENTREPARTICULIERS.COM ne veillait pas à recueillir le consentement préalable des personnes à recevoir des prospections commerciales par sms ou par courrier électronique, contrairement aux dispositions de l'article L.34-5 du code des postes et des communications électroniques.
La société ENTREPARTICULIERS.COM a affirmé, lors de l'audience du 20 mai 2008, avoir cessé toute campagne de prospection commerciale par sms ou par courrier électronique.

1. Sur le droit d'information des personnes

12. Le rapporteur avait indiqué que le formulaire du site « entreparticuliers.com » à partir duquel les clients saisissaient leurs données personnelles ne contenait aucune information répondant aux exigences de l'article 32 de la loi du 6 janvier 1978 modifiée.
La société ENTREPARTICULIERS.COM a communiqué à la CNIL, lors de l'audience du 20 mai 2008, une charte relative à la protection des données à caractère personnel dans laquelle sont précisés l'identité du responsable de traitement, les finalités de la collecte des données à caractère personnel, les destinataires de ces données, leurs durées de conservation ainsi que

les droits d'accès, de modification et de suppression des données à caractère personnel des annonceurs. Elle figure sur le site Internet de la société et les formulaires d'inscription y font référence.
13.Si la société ENTREPARTICULIERS.COM a pris plusieurs mesures correctives afin de respecter les dispositions de la loi « informatique et libertés », elles n'en demeurent pas moins tardives, voire pas encore effectives, s'agissant notamment du dispositif de paiement sécurisé prévu pour le mois de juin 2008.
14. Les observations en réponse formulées par la société ENTREPARTICULIERS.COM ne sont pas de nature à supprimer de manière rétroactive les faits constatés lors de la mission de contrôle, qui constituent de graves manquements aux articles 6, 32, 34, 39 et 40 de la loi du 6 janvier 1978 modifiée.

1. Sur le droit de suppression des personnes

15. Dans le rapport de sanction, il était indiqué que la société ENTREPARTICULIERS.COM n'avait mis en place aucune procédure permettant de garantir la prise en compte, de manière efficace, du droit de suppression des personnes prévu à l'article 40 de la loi du 6 janvier 1978 modifiée, plus particulièrement de celui de M. S qui s'est plaint auprès de la Commission de la conservation de ses informations bancaires dans les fichiers de la société.
La société ENTREPARTICULIERS.COM a communiqué à la CNIL un courrier adressé à M. S lui indiquant que les services de la société ont procédé à la suppression de ses coordonnées bancaires.
Aucune information n'a été apportée, lors de l'audience, concernant la procédure mise en place pour gérer de manière générale le droit de suppression des clients de la société.
PAR CES MOTIFS, conformément à l'article 45 de la loi du 6 janvier 1978 modifiée, la CNIL décide de :

- prononcer à l'encontre de la société ENTREPARTICULIERS.COM un avertissement ;
- publier la présente décision sur son site internet et sur la base « Légifrance ».

Le Président

Alex TURK