DONNÉES PERSONNELLES

Prospection commerciale : la CNIL sanctionne le défaut de consentement

La startup Nestor a été sanctionnée par la Cnil à la suite de plaintes pour non-respect du recueil du consentement des prospects lors de l'envoi d'offres commerciales par emails.

Spécialisée dans la livraison de repas en entreprise, la société Nestor s'est retrouvée dans le collimateur de la Cnil à la suite de plaintes pour non-respect du recueil du consentement des prospects lors de l'envoi d'offres commerciales par emails.

Qui n'a jamais reçu d'emails de prospection même après avoir explicitement refusé de recevoir ce type de communications commerciales de sites marchands ?

Très intrusive, la publicité par voie électronique est encadrée par un certain nombre de règles dont celles issues du code des postes et des communications électroniques (CPCE) et du règlement général sur la protection des données (UE) 2016/679 du 27 avril 2016 (RGPD) que la Commission nationale de l'informatique et des libertés (CNIL) veille à faire respecter.

Depuis l'entrée en vigueur du RGPD le 25 mai 2018 les procédures de contrôles et les sanctions de la Cnil se poursuivent.

Ces contrôles surviennent notamment à la suite d'instructions de plaintes de violation de données personnelles donnant lieu à l'ouverture de procédures formelles de contrôle.

C'est dans ce contexte que la Cnil a contrôlé la société Nestor en mai 2019 et en février 2020 en procédant à des vérifications en ligne sur son site internet et son application mais aussi sur place dans ses locaux. Ces opérations ont mis en exergue quatre manquements aux obligations prévues par le CPCE et le RGPD.

Le premier manquement reproché à la société Nestor vise l'obligation de recueillir le consentement des personnes lors d'une sollicitation commerciale envoyée par email.
L'article L 34-5 du CPCE interdit « *la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen* ». Il convient pour les professionnels, avant tout envoi d'une prospection commerciale par voie électronique, de recueillir le consentement du destinataire à recevoir de tels emails.
Or, pour constituer sa base de prospects, la société Nestor avait récupéré des données à caractère personnel accessibles en ligne qu'elle a ensuite confiées à deux sociétés tierces en charge d'établir des listes de prospection contenant les noms et prénoms de prospects et de rechercher des adresses électroniques professionnelles des personnes listées.
Une troisième société procédait à l'envoi des emails de prospection. Par ce procédé, 635 033 prospects ont reçu depuis 2017 des emails de prospection de la société de livraison de déjeuners.

La société Nestor aurait dû obtenir le consentement des personnes avant d'envoyer des offres commerciales sachant que les courriels ont été envoyés à des personnes non-clientes.

Le recueil du consentement doit s'exprimer par un moyen simple et spécifique, comme par exemple une case à cocher. Le consentement est exclu en cas de silence ou de case pré-cochée.

Face à ce comportement litigieux, la Cnil a enjoint la société Nestor de supprimer toutes les données collectées sans consentement des personnes concernées.

La simple mise à jour de l'application et du site internet ne permet pas de justifier la suppression des données collectées sans consentement.
Par ailleurs, la société Nestor a failli à l'obligation d'informer les personnes en application des articles 12 et 13 du RGPD.

L'article 12 du RGPD prévoit la transparence des informations et communications et les modalités de l'exercice des droits de la personne concernée tandis que l'article 13 détaille les informations à fournir lorsque les données personnelles sont collectées, à savoir :

- l'identité et coordonnées du responsable de traitement,
- la finalité et la base juridique du traitement des données à caractère personnel,
- les destinataires des données personnelles,
- s'il existe un transfert des données personnelles en dehors de l'Union européenne,
- la durée de conservation des données personnelles,
- les droits des personnes concernées,
- le droit d'introduire une réclamation auprès de l'autorité de contrôle,
- le caractère obligatoire ou facultatif de la collecte des données à caractère personnel,
- l'existence d'une décision automatisée,
- les traitements mis en place ultérieurement,
- l'origine des données quand elles ne sont pas collectées directement auprès de la personne.

Contrairement à ces obligations, le formulaire d'inscription au site internet nestorparis.com ne comportait pas ces informations.

Le site comportait tout de même une politique de confidentialité mais incomplète et imprécise à plusieurs égards, qu'il s'agisse en particulier des durées de conservation des données à caractère personnel ou de la possibilité de transmission des données à des partenaires. L'application mobile n'était pas mieux lotie puisqu'aucune information relative à la protection des données à caractère personnel n'était transmise aux utilisateurs créant un compte.

Parant à ces manquements en cours de procédure, la société Nestor s'est mise en conformité en insérant dans le formulaire d'inscription sur le site internet et sur l'application un lien vers la politique de confidentialité exhaustive.

Ensuite, la Cnil reprochait à la société Nestor de n'avoir pas respecté l'obligation du droit d'accès des personnes prévue à l'article 15 du RGPD. Cette obligation vise pour la personne concernée à obtenir du responsable du traitement l'accès aux données personnelles à son sujet notamment la finalité du traitement, les catégories de données traitées, les destinataires ainsi que leur source lorsque ces données n'ont pas été collectées auprès de la personne concernée.

Dans la réponse à apporter par le responsable de traitement, si la demande est électronique, la réponse doit être électronique. La copie des données personnelles ne doit pas comporter les données d'une autre personne ou porter atteinte aux droits et libertés d'autrui.

Les manquements ont été mis en lumière par deux plaignants reprochant d'une part à la société Nestor de ne leur avoir pas fourni une copie de leurs données à caractère personnel. D'autre part, elle n'avait pas donné d'explications quant à la source des données les concernant obtenues indirectement. La société Nestor avait répondu que partiellement aux demandes d'accès formulées indiquant simplement pour un des plaignants sa désinscription des listes de diffusion.

Enfin, le dernier manquement portait sur l'obligation d'assurer la sécurité des données à caractère personnel en application de l'article 32 du RGPD.

Cet article vise les 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 y aient accès, par exemple : « *la pseudonymisation, le chiffrement des données à caractère personnel, les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des système et services de traitement, des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celle-ci dans des délais appropriés en cas d'incident physique ou technique (...)* ».

Les critères d'exigences du mot de passe du site internet et de l'application étaient en cause. Pour la création d'un compte sur le site internet, un mot de passe de six caractères était accepté et sur l'application, un mot de passe d'un caractère, ce qui était d'évidence insuffisant.

La Cnil rappelle dans sa délibération les critères de base d'un mot de passe fort comportant au minimum douze caractères et au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. Pour un mot de passe ne contenant que huit caractères, la Cnil recommande de prévoir une mesure complémentaire comme le blocage du compte après plusieurs échecs de connexion ou la mise en place de mécanismes de contrôle tel que le test « *Captcha* ».

Ainsi, le responsable de traitement doit pouvoir garantir une sécurité externe, interne, technique et organisationnelle adaptée au risque.

La Cnil met à la disposition un guide sur la sécurité des données personnelles permettant d'aider les professionnels pour leur mise en conformité (https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles).

Face aux manquements identifiés par la Cnil, les sanctions prononcées ont pris en compte la gravité des violations en cause mais aussi la bonne foi de la société Nestor qui a mis en place des mesures correctrices en cours de procédure.

Pour sanctionner les deux premiers manquements, considérant la gravité de l'absence de recueil du consentement des prospects pour la constitution de sa base clients, du nombre important de personnes concernées et du caractère essentiel des obligations d'information et de transparence, la Cnil a prononcé une amende de 20.000 euros.

Le montant peut paraître dérisoire par rapport au montant maximum pouvant être retenu à savoir 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Pour fixer l'amende, la Cnil a pris en compte la situation économique de la société mais aussi la crise sanitaire de la Covid-19.

Outre cette amende, la Cnil a prononcé des injonctions de mise en conformité lorsque les manquements n'avaient pas été corrigés, tel que la suppression de la base de données des personnes n'ayant pas consenti à la réception des sollicitations commerciales par emails de la société Nestor.
Enfin dans son arsenal de sanction, la Cnil a décidé d'une mesure de publicité de la délibération justifiée par la gravité des manquements relevés.

Cette dernière sanction, dont l'impact en termes d'image et de réputation n'est pas anodin, tend à rééquilibrer le faible montant de la sanction pécuniaire.

Mélanie ERBER
Avocat associé

Marion FAUPIN
Avocat
Coblence avocats

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info