

DATA SCRAPING : UNE LIMITATION FERME AUX PRATIQUES DE MARKETING DIRECT PAR LA CNIL

Date: 10 March 2021

French IP/IT Alert

By: Claude-Étienne Armingaud, Alexia Montagnon, Clara Schmit

La Commission Nationale de l'Informatique et des Libertés ([CNIL](#)) a clôturé l'année 2020 avec une amende de 20 000 euros à l'encontre la société française NESTOR spécialisée dans la préparation et la livraison de repas sur le lieu de travail (voir la décision complète [ici](#)).¹

Plusieurs violations du Règlement Général sur la Protection des Données (« RGPD »)² et la Directive Vie privée et Communications électroniques (« [Directive ePrivacy](#) ») concernant le traitement des données à caractère personnel des clients et prospects ont été relevés par la CNIL, et notamment :

- L'absence de consentement préalable des prospects à recevoir une communication électronique à des fins de marketing direct, en violation de l'[Article L.34-5 du Code des Postes et des Communications Électroniques \(« CPCE »](#))³;
- Le manquement à l'obligation d'informer correctement les personnes concernées,⁴ soit :
 - Lors de la création de leur compte sur la plateforme de la société ;
 - Lors de la collecte indirecte de données via des sources externes.
- L'incapacité à traiter correctement les demandes d'accès des personnes concernées.⁵

Si l'amende apparaît relativement limitée au regard du montant maximal de 20 millions d'euros ou de 4% du chiffre d'affaires pouvant être prononcé, cette décision reste une opportunité d'examiner de plus près les pratiques de web scraping et de marketing direct qui se développent rapidement.

DATA SCRAPING ET PROTECTION DES DONNÉES PERSONNELLES

La société Nestor a constitué sa base de données de clients potentiels au travers de la collecte automatisée de données à caractère personnel rendues publiques au travers d'une plateforme tierce, une pratique connue sous le nom de "data scraping" ou "web scraping", utilisée massivement par les start-up et les entreprises émergentes pour accélérer leurs campagnes de marketing.

Cette base de données, comprenant 635 033 contacts, avait été établie à l'aide de plusieurs services successivement fournis par des tiers :

- Les données à caractère personnel étaient initialement collectées par le biais du logiciel « Sales Navigator » édité par LinkedIn, qui répertorie toutes les personnes travaillant dans une entreprise et dans une région donnée ;

- Une deuxième société était ensuite chargée d'ajouter les adresses électroniques professionnelles de ces personnes ; et
- Une troisième société envoyait enfin des courriels de prospection pour le compte de la société NESTOR.

En vertu de l'[Article 13.1 de la Directive ePrivacy](#), une telle pratique aurait nécessité le consentement de la personne concernée, selon les modalités prévues par le RGPD,⁶ avant l'envoi d'une communication de marketing direct par voie électronique. En effet, la Directive ePrivacy interdit les pratiques de marketing direct effectuées par des « moyens électroniques » (c'est-à-dire les courriers électroniques, les messages textuels, les télécopieurs ou les automates d'appel),⁷ sauf si ces pratiques sont le fait de l'entité qui a effectivement collecté directement les données à caractère personnel en premier lieu, dans le cadre de la vente d'un produit ou de la fourniture d'un service, et visent à offrir des produits et services analogues.

Cet article de la Directive ePrivacy a ensuite été transposée en droit français dans l'[Article L.34-5 CPCE](#).

Étant donné que la société NESTOR collectait les données personnelles non pas auprès des personnes concernées elles-mêmes, mais via le logiciel de LinkedIn, un consentement préalable était donc nécessaire.

En outre, les entreprises utilisant des données à caractère personnel collectées indirectement entrent également dans le champ d'application de l'[Article 14 RGPD](#), qui impose de fournir certaines informations aux personnes concernées, dans un délai maximum de 30 jours suivant la fourniture (ou la collecte) de leurs données à caractère personnel.

L'ARRÊT NESTOR : L'ORIGINALITÉ DE LA BASE LÉGALE

Bien que la Directive ePrivacy ait été transposée différemment dans plusieurs États membres de l'UE (et en attendant son successeur, le Règlement ePrivacy, pour harmoniser ce domaine), l'interprétation de la CNIL peut avoir des conséquences à l'échelle européenne pour toutes les entreprises.

Plus particulièrement, certains États membres de l'UE ont choisi d'interpréter strictement la Directive ePrivacy et d'imposer le recueil du consentement de toutes les personnes concernées.

D'autres ont prévu une exemption dans le contexte des relations B2B, où le consentement n'est donc pas nécessaire. À cet égard, l'exception française prend la forme d'une page web unique (non contraignante et susceptible d'être modifiée à tout moment) sur le site internet de la CNIL, indiquant qu'une information préalable et un droit d'opposition sont suffisants en cas de marketing direct à destination de professionnels.

La société NESTOR a fondé sa défense sur cette exemption, arguant du fait qu'aucun consentement préalable n'était exigé et qu'elle pouvait, au contraire, s'appuyer sur son intérêt légitime comme base légale à ses pratiques de marketing direct par voie électronique.

Néanmoins, la CNIL n'a pas suivi ce raisonnement : la Commission a estimé que des messages concernant la livraison de repas sur le lieu de travail n'avaient que peu de rapport avec l'activité professionnelle effective des prospects, même si ces repas ont bien lieu au cours de leur activité professionnelle. Selon la CNIL, un lien direct entre l'opération de marketing et l'activité professionnelle du prospect est nécessaire pour pouvoir se fonder sur l'intérêt légitime.

D'autres facteurs aggravants ont été relevés, comme le manque d'information des personnes concernées sur les opérations de traitement des données et l'impossibilité de s'opposer à une telle collecte.

Cette décision a été publiée six mois après que la CNIL a publié sa position sur la collecte de données personnelles accessibles au public (voir notre précédente Alerte en anglais [ici](#)) et constitue un rappel important sur le fait que la simple disponibilité des données en ligne ne saurait, à elle seule, justifier de leur collecte et de leur réutilisation sans les diligences nécessaires. En outre, en sus des préoccupations relatives à la protection des données, le data scraping peut également être soumis à des restrictions supplémentaires en vertu du droit de la propriété intellectuelle et du droit sui generis sur les bases de données.

POURQUOI CETTE DÉCISION EST-ELLE IMPORTANTE ?

Cette décision peut sembler anecdotique compte tenu de l'amende prononcée. Néanmoins, son importance n'est pas fondée uniquement sur le faible montant de l'amende, mais plutôt sur l'objet même de la décision : elle constitue une limitation ferme de la CNIL à la pratique du web scraping à des fins de marketing direct, via des plateformes tierces, telles que LinkedIn, et pourrait également indiquer que l'exemption prévue pour les relations B2B pourrait prendre fin, du moins dans sa version actuelle.

Afin de renforcer la portée de cet arrêt, la CNIL a décidé de rendre publique cette décision et a également fourni un article très complet sur son site Internet, détaillant les différents manquements commis par la société.

La portée de cette décision est d'autant plus importante que la CNIL a adopté, le jour précédant sa décision à l'encontre de NESTOR, le 7 décembre 2020, une autre décision contre la société [PERFORMECLIC](#)⁸ qui portait également sur les pratiques de marketing direct et de collecte indirecte (sans recours toutefois au data scraping). Cela semble indiquer que la réalisation d'enquêtes plus approfondies sur les pratiques de marketing direct est une propriété pour la CNIL cette année. L'équipe Data Protection de K&L Gates se tient à votre disposition pour vous aider à assurer la conformité de vos activités de marketing direct dans l'Union Européenne.

FOOTNOTES

¹ [CNIL, Décision SAN-2020-018, 8 Décembre 2020.](#)

² Règlement (UE) No. 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE ([Règlement Général sur la Protection des Données](#)).

³ [Article L.34-5 du Code des Postes et des Communications Électroniques.](#)

⁴ [Article 12 et 13 RGPD.](#)

⁵ [Article 15 RGPD.](#)

⁶ Comme le souligne [l'Avis du Conseil Européen de Protection des Données \("CEPD"\) relative aux interactions entre la Directive ePrivacy \("Vie privée et communications électroniques"\) et le RGPD](#), lorsque le consentement est requis en vertu de la Directive ePrivacy, le consentement est nécessairement requis comme base légale en vertu du RGPD.

⁷ Elle ne limite pas, néanmoins, le marketing par voie postale ou les appels téléphoniques direct avec des opérateurs humains.

⁸ [CNIL, Décision SAN-2020-016, 7 Décembre 2020.](#)

KEY CONTACTS



CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.