Délibération SAN-2020-018 du 8 décembre 2020

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Sanction
Etat juridique : En vigueur
Date de publication sur Légifrance : Mercredi 06 janvier 2021

Délibération de la formation restreinte n°SAN-2020-018 du 8 décembre 2020 concernant la société NESTOR SAS

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Philippe-Pierre CABOURDIN, vice-président, Mme Dominique CASTERA, Mme Anne DEBET et Mme Christine MAUGÜE, membres ;

Vu la Convention no 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 le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, notamment ses articles 20 et suivants ;

Vu l'ordonnance no 2020-306 du 25 mars 2020 relative à la prorogation des délais échus pendant la période d'urgence sanitaire ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu les saisines nos […], […], […], […] et […] ;

Vu la décision n° 2019-082C du 24 avril 2019 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 des traitements mis en œuvre par cet organisme ou pour le compte de la société NESTOR ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 19 décembre 2019 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société NESTOR le 28 février 2020 ;

Vu les observations écrites versées par la société NESTOR le 21 août 2020 ;

Vu la réponse du rapporteur à ces observations notifiée le 18 septembre 2020 au conseil de la société ;

Vu les nouvelles observations écrites versées par le conseil de la société NESTOR, reçues le 16 octobre 2020, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu la procédure interne de gestion des demandes d'exercice des droits versée par le conseil de la société NESTOR le 6 novembre 2020 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 5 novembre 2020 :

Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société NESTOR :

[…] ;

[…] ;

[…] ;

[…] ;

[…].

La société NESTOR ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I.Faits et procédure

La société NESTOR SAS (ci-après la société) est une société par actions simplifiée créée en février 2015, qui a pour activité la préparation et la livraison de repas à destination d'employés de bureaux, commandés à partir du site web de la société nestorparis.com et d'une application mobile. Son siège social est situé 113, rue Victor Hugo à Levallois-Perret (92300).

En 2018, la société NESTOR SAS a réalisé un chiffre d'affaires d'environ […] d'euros et un résultat net négatif d'environ […] d'euros. En 2019 la société a réalisé un chiffre d'affaires d'environ […] d'euros et un résultat net négatif d'environ […] d'euros. La société NESTOR emploie environ 74 personnes. Le 14 mai 2019, la société recensait 169 768 comptes clients créés via son site et son application mobile.

En novembre 2018 et janvier 2019, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été saisie de quatre plaintes par des personnes non clientes de la société, indiquant avoir reçu des courriels de prospection de la part de cette dernière sans qu'elles aient fourni leur consentement préalable (saisines n° […], […], […] et […]). Ces courriels contenaient des informations relatives à des offres commerciales et aux menus proposés par la société. Certains plaignants informaient la CNIL que la société leur avait indiqué avoir reconstitué leur adresse électronique, afin de les contacter, sur la base du format de l'adresse électronique de leur entreprise à partir des données diffusées sur le réseau social professionnel de la société […].

Par ailleurs, une plaignante indiquait qu'elle rencontrait des difficultés à s'opposer au traitement de ses données caractère personnel par la société à des fins de prospection par courrier électronique (saisine n°[…]). Plusieurs plaignant indiquaient également que malgré leur désinscription de la newsletter reçue par courriel, ils continuaient à recevoir des messages de prospection par ce biais.

Enfin, deux plaignants indiquaient avoir demandé, en vain, à la société, une copie des données à caractère personnel les concernant traitées par celle-ci, ainsi que plusieurs informations relatives à la finalité du traitement, aux destinataires des données, aux durées de conservation des données ou encore à la source de leurs données (saisines n° […] et […]).

Le 3 mai 2019, en application de la décision no 2019-082C de la présidente de la CNIL, une délégation de la CNIL a procédé à une mission de contrôle en ligne, sur le site web et l'application mobile mis en œuvre par la société. Cette mission a eu pour objet de vérifier le respect par cette société de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement ou le RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi du 6 janvier 1978 modifiée ou la loi Informatique et Libertés).

Au cours de cette mission de contrôle, la délégation a suivi le parcours d'inscription d'une personne sur le site web ainsi que sur l'application mobile de la société et a créé un compte au nom de la CNIL. Elle a ainsi effectué des vérifications en lien avec les données renseignées par les personnes lors de leur inscription, les informations relatives à la protection des données à caractère personnel fournies aux personnes concernées ainsi que les mesures de sécurité mises en place par la société s'agissant des mots de passe associés aux comptes.

Le 14 mai 2019, une délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société, en application de la décision n° 2019-082C précitée. Lors de ce contrôle, la société a indiqué à la délégation qu'elle procédait à la refonte de son site web afin de se conformer au RGPD, s'agissant notamment de l'information des personnes et des moyens d'opposition à la réception de la lettre d'information. La société a également expliqué à la délégation la manière dont elle constitue sa base de données de prospects. Des vérifications ont enfin été effectuées en ce qui concerne les suites apportées aux plaintes dont la CNIL a été saisie, s'agissant des droits d'accès et d'opposition des personnes.

En réponse à une demande du 21 juin 2019, la société a fourni à la délégation de contrôle de la CNIL, par courriel du 3 juillet suivant, des informations relatives à la source des données à caractère personnel contenues dans sa base de prospects. Enfin, par courriel du 11 septembre 2019, la société a fourni à la CNIL des éléments relatifs à la base légale du traitement mis en œuvre à des fins de prospection commerciale, au droit d'opposition ainsi qu'aux durées de conservation des données des prospects et clients.

Aux fins d'instruction de ces éléments, la présidente de la Commission a désigné Monsieur François PELLEGRINI en qualité de rapporteur, le 19 décembre 2019, sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée dans sa version applicable au jour de la désignation.

Le 20 février 2020, aux fins d'actualiser les constatations déjà effectuées, une délégation de la CNIL a procédé à une nouvelle mission de contrôle en ligne du site nestorparis.com et de l'application mobile de la société. La délégation a de nouveau créé un compte au nom de la Commission, sur le site web et l'application mobile, et a effectué des vérifications relatives à la transparence des informations fournies aux personnes ainsi qu'à la robustesse des mots de passe associés aux comptes.

À l'issue de son instruction, le rapporteur a fait notifier à la société NESTOR SAS, le 28 février 2020, un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce.

Ce rapport proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité le traitement avec les dispositions des articles L. 34-5 du Code des postes et des communications électroniques (ci-après le

CPCE) et 12, 13, 15 et 32 du Règlement, assortie d'une astreinte de cinq cents euros par jour de retard à l'issue d'un délai de trois mois suivant la notification de la délibération de la formation restreinte, ainsi qu'une amende administrative. Il proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

Était également jointe au rapport une convocation à la séance de la formation restreinte du 7 mai 2020 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites en application des dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019.

Le 11 mars 2020, par l'intermédiaire de son conseil, la société NESTOR sollicitait par courrier motivé, un délai pour produire ses observations. Par courriel du 18 mars 2020, le président de la formation restreinte a informé la société NESTOR qu'elle pouvait produire ses observations en défense jusqu'au 20 avril 2020.

Le 8 avril 2020, en vertu de l'ordonnance n° 2020-306 du 25 mars 2020 relative à la prorogation des délais échus pendant la période d'urgence sanitaire et à l'adaptation des procédures pendant cette même période, prise en application de la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de Covid-19, le président de la formation restreinte a informé la société qu'elle disposait d'un délai supplémentaire pour produire ses observations au rapport du rapporteur, jusqu'au 24 août 2020.

Le 21 août 2020, par l'intermédiaire de son conseil, la société a produit des observations. Le rapporteur y a répondu le 18 septembre suivant.

Le 10 septembre 2020, les services de la Commission ont adressé à la société une convocation à la séance de la formation restreinte du 5 novembre 2020.

Par courrier électronique du 25 août 2020, sur le fondement de l'article 40, alinéa 4, du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés (ci-après le décret du 19 mai 2019), le rapporteur a demandé au président de la formation restreinte un délai supplémentaire de quinze jours pour répondre aux observations de la société, qui lui a été accordé le 27 août 2020. La société en a été informée le même jour.

Le 16 octobre, la société a produit de nouvelles observations en réponse à celles du rapporteur.

La société et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte du 5 novembre 2020.

II.Motifs de la décision

A.Sur la régularité de la procédure

1.Sur le grief tiré de l'absence de pouvoirs de la formation restreinte

La société considère que la formation restreinte ne dispose du pouvoir de prononcer les mesures visées à l'article 20 III de la loi Informatique et Libertés qu'en présence de manquements persistants.

En premier lieu, elle soutient que cette analyse découle de l'interprétation des termes de la loi, l'article 20 III de la loi Informatique et Libertés prévoyant la possibilité pour la formation restreinte d'avoir recours aux mesures prévues à l'article précité lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi .

Le rapporteur soutient que l'interprétation de l'article 20 III de la loi Informatique et Libertés présentée par la société ne saurait être suivie. Le législateur a entendu permettre à la formation restreinte de la CNIL de prononcer une sanction, notamment pécuniaire, y compris en cas de manquement dûment constaté mais pour lequel une mise en demeure serait sans objet, le manquement ayant cessé et n'appelant plus de correction.

La formation restreinte considère que les mesures prises par un responsable de traitement pour faire cesser un manquement constaté, si elles justifient qu'aucune mise en demeure ou aucune injonction ne lui soient adressées pour l'avenir, ne la privent pas de la possibilité de prononcer une mesure correctrice, et notamment une amende administrative, dans la mesure où la mise en conformité du responsable de traitement n'a pas pour effet de faire disparaître l'existence de manquements passés.

Elle souligne que cette interprétation de l'article 20 de la loi Informatique et Libertés est dans la ligne du RGPD en ce que cet article vise à la responsabilisation des responsables de traitement. Les mesures correctrices relevant des pouvoirs de la formation restreinte de la CNIL peuvent être prises directement dans tous les cas, que le manquement puisse toujours, ou non, faire l'objet d'une mise en conformité. Le considérant 148 du RGPD précise ainsi que toute violation du présent règlement peut faire l'objet de sanctions : Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. […]. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation […] . Le critère de durée de la violation s'applique donc aussi bien à un manquement terminé que persistant.

Par ailleurs, la formation restreinte observe que le Conseil d'Etat a retenu cette interprétation en rappelant que : Il résulte de ces dispositions, éclairées par les travaux préparatoires de la loi du 7 octobre 2016, que la formation restreinte de la CNIL peut, sans mise en demeure préalable, sanctionner un responsable de traitement dont les manquements aux obligations qui lui incombent ne sont pas susceptibles d'être régularisés, soit qu'ils soient insusceptibles de l'être, soit qu'il y ait déjà été remédié. (CE, n° 423559, 17 avril 2019, Association pour le développement des foyers).

En second lieu, la société soutient que l'absence de règles de prescription des manquements dans la loi Informatique et Libertés et le RGPD démontre que seuls des manquements en cours au jour de la séance de la formation restreinte peuvent être sanctionnés et qu'une interprétation contraire se heurterait à la jurisprudence retenue par la Cour européenne des droits de l'homme selon laquelle les règles de prescription sont une condition du procès équitable.

Le rapporteur rappelle que la Commission a été saisie de quatre plaintes entre 2018 et 2019, que des contrôles ont été effectués par la délégation de la CNIL en mai 2019 et en février 2020 et que le rapporteur désigné en décembre 2019 aux fins d'instruction de ces éléments a notifié son rapport le 28 février 2020. La formation restreinte considère donc que la Commission a appliqué un délai raisonnable entre les constats effectués par la délégation de contrôle et la saisine de la formation restreinte.

La formation restreinte relève à cet égard qu'il résulte de la jurisprudence de la Cour de justice de l'Union européenne que l'obligation de l'administration d'agir dans un délai raisonnable, dont le respect est susceptible d'être contrôlé par le juge de l'Union, offre un niveau de protection suffisant dans les situations où aucun délai de prescription n'est fixé par les textes. (CJUE, n° T-342/14, Ordonnance du Tribunal, CR contre Parlement européen et Conseil de l'Union européenne, 12 décembre 2014).

La formation restreinte considère ainsi que la société n'est pas fondée à soutenir qu'elle ne dispose du pouvoir de prononcer les mesures visées à l'article 20 III de la loi Informatique et Libertés qu'en présence de manquements persistants et actuels, et que la procédure suivie devant elle méconnait le droit à un procès équitable.

2. Sur le grief tiré de la méconnaissance du champ de la saisine de la formation restreinte

La société considère que la formation restreinte ne peut se prononcer sur le manquement allégué aux dispositions de l'article L. 34-5 du code des postes et des communications électroniques (ci-après le CPCE).

En premier lieu, la société soutient que la décision de contrôle n° 2019-082C de la présidente de la CNIL, les actes d'investigation ou d'instruction qui ont suivi, ainsi que la décision de la présidente du 19 décembre 2019 portant désignation d'un rapporteur et saisine de la formation restreinte, ne visent pas l'article L. 34-5 du CPCE. En conséquence, la formation restreinte ne pourrait se prononcer sur le manquement allégué aux dispositions de l'article L. 34-5 du CPCE sans méconnaître le champ de sa saisine.

La société soutient également que la formation restreinte ne peut se fonder sur les éléments de l'enquête pour établir un manquement à l'article L. 34-5 du CPCE sans méconnaître les principes de spécialité de l'enquête – imposant que l'enquête soit réalisée dans les limites de son champ défini par la décision qui en constitue la base juridique – et de loyauté de l'enquête – obligeant les enquêteurs à mentionner l'objet et la base juridique des investigations.

Le rapporteur rappelle que les décisions précitées visent la loi Informatique et Libertés et le RGPD et que les actes d'investigation ou d'instruction qui en résultent sont menés dans ce cadre. L'article 8 de la loi fixe les missions de la CNIL et précise notamment qu'elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France .

Le rapporteur soutient ainsi que la loi du 6 janvier 1978 modifiée renvoie à toutes les dispositions relatives à la protection des données à caractère personnel prévues par les textes législatifs et réglementaires. Les opérations de prospection visées par l'article L. 34-5 du CPCE concernent un traitement de données à caractère personnel et cet article donne compétence à la CNIL pour veiller à son respect lorsque les données traitées ont un caractère personnel. L'alinéa 6 de l'article L. 34-5 du CPCE prévoit ainsi que : La Commission nationale de l'informatique et des libertés veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'un abonné ou d'une personne physique, au respect des dispositions du présent article en utilisant les compétences qui lui sont reconnues par la loi n° 78-17 du 6 janvier 1978 précitée .

La formation restreinte considère que c'est dans ce cadre que la délégation de la CNIL a procédé à trois contrôles auprès de la société et que la formation restreinte a été saisie.

La formation restreinte souligne en outre que cette interprétation a été retenue par le Conseil d'Etat qui a reconnu la compétence de la CNIL pour veiller au respect des dispositions de l'article L. 34-5 du CPCE (CE, n° 368624, 11 mars 2015, Société TUTO4PC).

En conséquence, la formation restreinte a été régulièrement saisie et c'est sans méconnaitre les principes de spécialité et de loyauté qu'elle se fonde sur les éléments des contrôles pour examiner les faits commis par la société au regard des dispositions de l'article L. 34-5 du CPCE.

En second lieu, la société soutient que, si la formation restreinte pouvait être saisie de manquements allégués à l'article L. 34-5 du CPCE, les enquêteurs de la CNIL ne peuvent pas réaliser des mesures d'investigation à cet effet, cette prérogative étant réservée, en vertu de l'alinéa 7 de l'article L. 34-5 du CPCE, aux agents de la concurrence, de la consommation et de la répression des fraudes et aux fonctionnaires chargés de missions de protection économique des consommateurs.

Or, le rapporteur rappelle que les dispositions de l'alinéa 6 de l'article L. 34-5 du CPCE prévoient que la CNIL utilise ses compétences afin de veiller au respect de l'article précité pour ce qui concerne la prospection directe utilisant les coordonnées d'un abonné ou d'une personne physique. Ces compétences sont précisées dans la loi du 6 janvier 1978 modifiée et elles comportent, au titre de ses articles 19 et 20, des pouvoirs d'enquête et de sanction.

La formation restreinte considère ainsi que les agents de la CNIL sont compétents pour réaliser des missions de contrôle en vertu des dispositions de l'article L. 34-5 du CPCE afin de veiller au respect de cet article pour ce qui concerne précisément la prospection directe utilisant les coordonnées d'un abonné ou d'une personne physique.

3. Sur l'imprécision des griefs opposés à la société

La société souligne que les griefs notifiés dans le rapport de sanction ne sont délimités ni matériellement ni dans le temps et ne répondent pas au standard de preuve requis en matière pénale. En conséquence, la société soutient qu'elle n'est pas en mesure d'exercer utilement ses droits de la défense.

Le rapporteur indique que les faits sur lesquels les manquements ont été fondés ont été constatés lors des contrôles effectués par la délégation de la CNIL les 3 et 14 mai 2019 et le 20 février 2020. Ces manquements ont été matériellement et temporellement caractérisés dans le rapport notifié à la société. Le rapporteur estime ainsi avoir permis à la société d'exercer utilement ses droits de la défense.

Le rapporteur souligne également que la formation restreinte n'est pas une juridiction pénale et qu'elle dispose du pouvoir de prononcer des sanctions de nature administrative et qu'ainsi le standard de preuve requis devant la formation restreinte ne doit pas répondre aux exigences de la matière pénale mais à celles fixées par la loi Informatique et Libertés et par son décret d'application.

A cet égard, le rapporteur rappelle également que chaque grief est étayé par des éléments issus des opérations de contrôle dans le cadre desquelles un procès-verbal, comportant des pièces en annexe, est rédigé.

Au vu de l'ensemble de ces éléments, la formation restreinte considère que la délégation de contrôle a assuré un standard de preuve élevé qui permet de garantir leur fiabilité, que les manquements ont été matériellement et temporellement caractérisés dans le rapport notifié à la société et qu'ainsi, la société ne saurait se prévaloir d'une imprécision des griefs qui lui sont opposés.

B.Sur le manquement relatif à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un système automatisé de communications électroniques en application de l'article L. 34-5 du CPCE

1.Sur l'absence de consentement des personnes à la réception de messages de prospection commerciale

L'article L. 34-5 du CPCE dispose : Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen.

Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. […] .

Aux termes de l'alinéa 6 du même article, La Commission nationale de l'informatique et des libertés veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'un abonné ou d'une personne physique, au respect des dispositions du présent article en utilisant les compétences qui lui sont reconnues par la loi n° 78-17 du 6 janvier 1978 précitée. A cette fin, elle peut notamment recevoir, par tous moyens, les plaintes relatives aux manquements aux dispositions du présent article […] .

Le rapporteur soutient que la société ne recueille pas le consentement des personnes dont les données à caractère personnel sont accessibles sur Internet, préalablement à l'envoi de messages de prospection commerciale.

Le rapporteur a relevé que, lors du contrôle du 14 mars 2019, la société a indiqué à la délégation de contrôle de la CNIL qu'elle constitue sa base de prospects à partir de données à caractère personnel accessibles en ligne sur le site web de réseau social professionnel de la société [...]. Elle a précisé travailler avec deux sociétés, A et B, pour la création de bases de données à caractère personnel destinées à la prospection commerciale.

Tout d'abord, la société A établit des listes de prospection contenant les noms et prénoms de prospects, associés à la dénomination de l'entreprise au sein de laquelle ils travaillent. Ces données sont collectées par le service Sales Navigator proposé par la société [...], qui recense l'ensemble des personnes travaillant dans une entreprise et une région. Par la suite la société NESTOR transfère le fichier établi par la société A, à la société B, qui procède à l'enrichissement de ce fichier, notamment en ajoutant l'adresse électronique professionnelle des personnes.

La société a indiqué à la délégation de contrôle de la CNIL que les fichiers constitués à l'aide de ces deux sociétés lui permettent, par la suite, de solliciter les personnes susceptibles d'être intéressées par ses services. Pour ce faire, il revient enfin à une autre société, la société C, de procéder aux envois à ces prospects de courriels d'information et de codes promotionnels pour le compte de la société NESTOR.

La société a informé la délégation que, 635 033 prospects ont reçu, depuis 2017, de tels courriers électroniques de prospection.

La société soutient que la base légale du traitement ayant pour finalité la prospection commerciale des personnes, effectué sur leur adresse électronique professionnelle est l'intérêt légitime du responsable de traitement. La société a également précisé avoir pour ambition de devenir la référence des services de livraison de déjeuners d'affaires dans les locaux professionnels de ses clients et qu'il est donc vital pour elle d'acquérir une base de clients professionnels potentiels.

Le rapporteur a relevé que dans un premier temps, la société avait informé la délégation qu'elle ne recueillait pas le consentement des personnes dès lors que cet emailing de prospection – dont la base légale est l'intérêt légitime de NESTOR – intervient strictement dans le cadre professionnel que constituent les déjeuners en entreprise (adresse de

courriel professionnelle, livraison dans les locaux professionnels, aux heures d'exercice de l'activité professionnelle du client, etc.) .

Dans sa réponse au rapport de sanction, la société a ensuite soutenu qu'elle s'assurait du consentement des personnes à ce que leurs données à caractère personnel soient utilisées à des fins de ciblage publicitaire en choisissant les services de la société [...], dont la politique de confidentialité prévoit la communication des données à caractère personnel de ses membres à des annonceurs : En choisissant les services de la société [...], NESTOR a pris les précautions nécessaires pour s'assurer du consentement des prospects à ce que leurs données soient utilisées à des fins de ciblage publicitaire et à ce qu'elles soient communiquées à des annonceurs. En l'espèce, NESTOR recours aux services de la société [...] en tant que l'un de ses sous-traitants. La société [...] agit donc au nom et pour le compte de NESTOR qui peut donc légitimement se prévaloir du consentement recueilli par la société [...] pour son compte.

La formation restreinte relève que le réseau social professionnel [...] permet à des personnes de s'inscrire afin d'entrer en relation avec des professionnels, dans le cadre d'une recherche d'emploi, ou encore de partager des informations avec leur réseau professionnel et d'étendre ce réseau professionnel. La formation restreinte considère dès lors que les messages de prospection envoyés par la société pour la vente de repas sur le lieu de travail des personnes n'ont que peu de lien avec l'activité professionnelle des prospects.

La formation restreinte considère également que les prospects démarchés n'ont pas eu connaissance de la collecte de leurs données à caractère personnel par la société et qu'elle a procédé à une prospection par courriels et SMS, sans avoir préalablement recueilli leur consentement.

En outre, la formation restreinte souligne que la prospection commerciale réalisée par la société entre dans le champ de l'alinéa 1 de l'article L. 34-5 du CPCE qui prévoit une base légale spécifique fondée sur le consentement, écartant ainsi la possibilité de l'intérêt légitime comme base légale pour ces opérations de prospection.

Dans de telles circonstances, la formation restreinte considère que la société est tenue de recueillir le consentement préalable, libre, spécifique et informé des personnes à recevoir des messages de prospection directe par courrier électronique, conformément à l'article L. 34-5 du CPCE, ce qu'elle ne fait pas.

La formation restreinte considère que la suppression des données à caractère personnel collectées sans le consentement des personnes est nécessaire dans la mesure où ces données sont traitées en l'absence de base légale, les personnes concernées n'ayant pas donné leur consentement. Elle relève que la société lui a indiqué avoir détruit sa base contenant les données à caractère personnel des prospects, sans toutefois en justifier. Elle considère par ailleurs que la suppression des données des prospects qui sont aujourd'hui devenus des clients de la société n'est pas nécessaire.

Dans ces conditions, la formation restreinte considère que la société a méconnu les dispositions de l'article L. 34-5 du CPCE.

2. Sur l'absence de consentement des personnes créant un compte sur le site web ou l'application de la société, à la réception des messages de prospection commerciale

Le rapporteur soutient que la société ne recueille pas le consentement des personnes créant un compte sur son site web ou son application pour le traitement de leurs données à caractère personnel à des fins de prospection commerciale par courriers électroniques.

Le rapporteur a relevé que lors de la création d'un compte par la délégation de la CNIL sur le site web de la société, à l'occasion du contrôle effectué le 3 mai 2019, aucun procédé visant à recueillir le consentement à la collecte et au traitement des données à des fins de prospection commerciale par courriers électroniques n'était mis en place.

Le rapporteur a également relevé que la délégation de la CNIL, qui n'avait passé aucune commande ni donné un tel consentement, a reçu des courriels et des SMS de prospection de la part de la société. De tels envois ont continué jusqu'en août 2019 et sont reconnus par la société.

La formation restreinte considère que la société est tenue de recueillir le consentement préalable, libre, spécifique et informé des personnes créant un compte sur le site web ou sur l'application de la société, à recevoir des messages de prospection directe par courriers électroniques, conformément à l'alinéa 1 de l'article L. 34-5 du CPCE.

Dans le cadre de la procédure, la société a justifié avoir inséré un mode d'obtention du consentement à compter du 11 septembre 2019 sur le site internet et du 5 mars 2020 sur l'application, et sa mise en conformité avec l'article L. 34-5 du CPCE puisque dès la création d'un compte client sur le site web ou sur l'application NESTOR, l'utilisateur doit renseigner un formulaire d'inscription dont l'une des rubriques consiste à renseigner, notamment, son choix de recevoir par courriel les menus du jour, de la semaine, ou les offres spéciales en cochant l'un des cases correspondantes.

Dans ces conditions, la formation restreinte considère que le manquement à l'article L. 34-5 du CPCE est constitué, mais que la société s'est complètement mise en conformité à la date de clôture de l'instruction.

C.Sur le manquement relatif à l'obligation d'informer les personnes en application des articles 12 et 13 du RGPD

Aux termes de l'alinéa 1 de l'article 12 du RGPD : Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples […] .

L'article 13 du RGPD exige du responsable de traitement qu'il fournisse, au moment où les données sont collectées, les informations relatives à son identité et ses coordonnées, les finalités du traitement et sa base juridique, les destinataires ou les catégories de destinataires des données à caractère personnel, le cas échéant les transferts de données à caractère

personnel, la durée de conservation des données à caractère personnel, les droits dont bénéficient les personnes ainsi que le droit d'introduire une réclamation auprès d'une autorité de contrôle.

Le rapporteur relève que, tel qu'il ressort des constations effectuées lors du contrôle en ligne du 20 février 2020, l'information mise à disposition des utilisateurs du site et de l'application, n'était ni complète au sens de l'article 13 du Règlement ni aisément accessible au sens de l'article 12 du Règlement.

En défense, la société a indiqué avoir procédé à des rectifications, dans le cadre de la procédure, afin de délivrer une information conforme aux exigences du RGPD.

La formation restreinte rappelle que pour considérer qu'un responsable de traitement satisfait à son obligation de transparence, il convient notamment que l'information fournie soit aisément accessible pour les personnes concernées au sens de l'article 12 du Règlement.

Elle relève, à cet égard, que cette disposition doit être interprétée à la lumière du considérant 61 du Règlement, aux termes duquel : les informations sur le traitement des données à caractère personnel relatives à la personne concernée devraient lui être fournies au moment où ces données sont collectées auprès d'elle . En ce sens, elle partage la position du G29 présentée dans les lignes directrices sur la transparence au sens du Règlement, adoptées dans leur version révisée le 11 avril 2018 (ci-après les lignes directrices sur la transparence), qui rappelle que la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder .

En l'espèce, la formation restreinte relève que le formulaire de collecte des données à caractère personnel permettant de s'inscrire sur le site web de la société ne comportait pas l'ensemble des informations exigées par l'article 13 du RGPD ou ne renvoyait pas vers une page dédiée contenant la totalité des informations prévues par le RGPD. Ainsi, la formation restreinte relève qu'aucune information relative aux bases juridiques des traitements mis en œuvre, aux destinataires ou aux catégories de destinataires des données, à la durée de conservation de celles-ci ou encore l'existence du droit d'introduire une réclamation auprès d'une autorité de contrôle n'était fournie.

En outre, la formation restreinte considère que la politique de confidentialité présente en page d'accueil du site web était incomplète s'agissant de l'information relative aux durées de conservation des données à caractère personnel des prospects.

La formation restreinte considère également que la politique de confidentialité ne permet pas aux personnes de savoir, pour chaque traitement, quelle base juridique fonde celui-ci, ni l'intérêt légitime poursuivi par le responsable de traitement lorsqu'un traitement de données à caractère personnel est fondé sur cette base légale.

La formation restreinte considère en outre que la politique de confidentialité est imprécise s'agissant de l'information relative aux destinataires des données à caractère personnel puisqu'il est indiqué que les données peuvent être transmises à certains partenaires […] . La formation restreinte considère que si la société n'est pas tenue de fournir l'identité de l'intégralité des destinataires des données, elle doit cependant, au moins, informer les personnes des catégories de destinataires des données.

Enfin, la formation restreinte observe qu'aucune information relative à la protection des données à caractère personnel n'était fournie aux personnes créant un compte sur l'application mobile.

Elle relève néanmoins que, dans le cadre de la procédure, la société a justifié avoir pris des mesures de mise en conformité avec les articles 12 et 13 du RGPD.

Tout d'abord, concernant le formulaire d'inscription sur le site web, la société justifie avoir inséré dans le formulaire, un lien intitulé Vos données nominatives renvoyant à la politique de confidentialité. La société justifie également avoir mis en conformité sa politique de confidentialité qui contient à présent l'intégralité des informations exigées par l'article 13 du RGPD. Enfin, la société indique qu'elle a opéré une refonte de son application mobile depuis le 5 mars 2020, et que la page d'inscription et la page d'accueil de l'application proposent, depuis, un lien renvoyant vers la politique de confidentialité, qui contient également l'ensemble des informations exigées par l'article 13 du RGPD.

Dans ces conditions, la formation restreinte considère que le manquement aux articles 12 et 13 du RGPD est constitué, mais que la société s'était mise en conformité à la date de clôture de l'instruction.

D.Sur le manquement relatif à l'obligation de respecter le droit d'accès des personnes en application de l'article 15 du RGPD

L'article 15, alinéa 1, du RGPD prévoit que le droit pour une personne d'obtenir du responsable du traitement l'accès aux données à caractère personnel la concernant et notamment lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, tout information disponible quant à leur source .

Il est également prévu à l'alinéa 3 du même article que le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement .

Enfin l'article 12.4 du RGPD prévoit que le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande.

Lors de l'instruction de deux plaintes reçues par la CNIL (saisines n° […] et […]), il est apparu que la société a manqué à son obligation de fournir aux plaignants une copie des données à caractère personnel les concernant qu'elle détenait dans sa base de données, ainsi qu'une information relative à la source de ces données.

S'agissant de la première plainte (n° […]), la société soutient que postérieurement à la saisine de la CNIL par le plaignant, Monsieur X, elle lui aurait communiqué des éléments justificatifs précisant que la désinscription des listes avait été infructueuse du fait d'une redirection des courriels d'une seconde adresse courriel vers la première.

Concernant la seconde plainte (n° […]), la société soutient que, postérieurement à la saisine de la CNIL par le plaignant, Monsieur Y, elle lui aurait communiqué la source de ses données à caractère personnel. La société ajoute que la demande formulée par Monsieur Y était une demande de portabilité relevant de l'article 20 du RGPD et non une demande portant sur le droit d'accès relevant de l'article 15 du RGPD.

Dans le cadre de la procédure la société a fait valoir qu'elle n'avait pas compris le périmètre de ces deux demandes.

En premier lieu, la formation restreinte relève qu'il ressort de la plainte déposée par Monsieur X que ce dernier a demandé à la société, par courriel du 8 novembre 2018, qu'une copie de l'ensemble de ses données à caractère personnel lui soit adressée ainsi que des informations sur la source de ses données. La formation restreinte relève que la société a uniquement indiqué en retour à Monsieur X qu'il était bien désinscrit de ses listes de diffusion.

La formation restreinte relève ainsi qu'il ressort des réponses apportées par la société au plaignant qu'elle ne lui a pas communiqué une copie de ses données à caractère personnel, ni leur source, tel que cela lui était demandé.

En second lieu, la formation restreinte relève qu'il ressort de la plainte déposée par Monsieur Y que la société a répondu à sa demande d'accès du 14 décembre 2018 plus de cinq mois après, soit le 14 mai 2019.

La formation restreinte considère que la société n'a pas indiqué la source des données, mais s'est contentée de préciser à Monsieur Y avoir reconstitué son adresse électronique sur la base d'une autre adresse électronique sans lui indiquer pour autant que cette autre adresse électronique avait été obtenue via le réseau social professionnel [...]. Ainsi la société a seulement énuméré le type de données qu'elle traitait. La formation restreinte considère également qu'il était clair qu'il ne s'agissait pas d'une demande de portabilité, notamment en ce que Monsieur Y indiquait précisément dans son courriel adressé à la société le 14 décembre 2018 […] je souhaite introduire une demande d'accès au titre du règlement européen sur la protection des données (RGPD/GDPR) afin d'obtenir une copie de toute information que vous conservez à mon sujet, que ce soit sous forme informatisée ou manuelle, en relation avec mes informations […] . En tout état de cause, que ce soit une demande adressée à la société au titre de l'article 15 du RGPD ou sur le fondement de son article 20, la formation restreinte considère que la société n'y a pas fait droit puisqu'aucun jeu de données le concernant ne lui a été communiqué sous quelque format que ce soit.

Dans ces conditions, la formation restreinte considère que le manquement à l'article 15 du RGPD est constitué sur ces deux plaintes, bien que ces dernières ne démontrent pas un caractère structurel du manquement reproché à la société. La formation restreinte considère par ailleurs que la société ne s'était toujours pas mise en conformité à la date de clôture de l'instruction.

E.Sur le manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel en application de l'article 32 du RGPD

L'article 32 du Règlement dispose :

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. […].

Le rapporteur a relevé que lors du contrôle en ligne du 3 mai 2019, la délégation a constaté qu'un mot de passe composé d'un seul caractère était accepté lors de la création d'un compte par une personne via l'application mobile et qu'un mot de passe composé de six caractères était accepté lors de la création d'un compte via le site web de la société.

Lors du contrôle du 20 février 2020, le rapporteur a relevé que si la société avait pris des mesures permettant de renforcer la composition du mot de passe requis pour la création d'un compte sur le site web de la société, un mot de passe composé d'un seul caractère était toujours accepté pour la création d'un compte sur l'application mobile.

Le rapporteur soutient donc que le mot de passe de connexion des clients à leur espace personnel, accessibles depuis l'application mobile, était toujours d'une robustesse insuffisante pour assurer la sécurité des données à caractère personnel, car composé d'un seul caractère.

En défense, la société conteste le caractère délibéré de défaut de sécurité qui lui est reproché et indique avoir modifié les mesures relatives à la gestion des mots de passe de connexion aux comptes des utilisateurs sur son application mobile à l'occasion de la mise à jour de cette dernière, le 5 mars 2020.

La formation restreinte considère que la longueur et la complexité d'un mot de passe demeurent des critères élémentaires permettant d'apprécier la force de celui-ci. Elle relève à cet égard que la nécessité d'un mot de passe fort est également soulignée par l'Agence nationale de sécurité des systèmes d'information, qui indique qu' un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules .

À titre d'éclairage, la formation restreinte rappelle que pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, la CNIL recommande, dans sa délibération n° 2017-012 du 19 janvier 2017, que le mot de passe comporte au minimum douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou alors comporte au moins huit caractères - contenant trois de ces quatre catégories de caractères - s'il est accompagné d'une mesure complémentaire comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses.

En l'espèce, la formation restreinte considère, d'abord, qu'au regard des règles peu exigeantes encadrant leur composition, la robustesse des mots de passe admis par la société était trop faible, conduisant à un risque de compromission des comptes associés et des données qu'ils contiennent.

La formation relève toutefois que la société justifie avoir modifié les mesures relatives à la gestion des mots de passe de connexion aux comptes des utilisateurs.

En conséquence, la formation restreinte considère que le manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel est constitué mais qu'au vu des éléments apportés par la société au cours de la procédure, il n'y a pas lieu de prononcer une injonction.

III. Sur les mesures correctrices et leur publicité

Aux termes du III de l'article 20 de la loi du 6 janvier 1978 modifiée :

Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; […]

7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

L'article 83 du RGPD prévoit que Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives ,

En premier lieu, concernant le prononcé d'une amende administrative, la société soutient que la formation restreinte ne dispose pas du pouvoir de prononcer une amende pour un manquement à l'article L. 34-5 du CPCE. En outre, la société relève que les articles 20 de la loi du 6 janvier 1978 et 83 du RGPD n'indiquent aucun plafond d'amende applicable pour un manquement à l'article L. 34-5 du CPCE et ne précisent pas les critères à prendre en compte dans la détermination du montant de l'amende.

Comme la formation restreinte l'a préalablement démontré, l'alinéa 6 de l'article L. 34-5 du CPCE donne pleinement compétence à la CNIL pour veiller à son respect pour la matière qui la concerne en usant des compétences qui lui sont reconnues par la loi Informatique et Libertés .

L'article 20, paragraphe III, point 7) de la loi du 6 janvier 1978 modifiée précise que la CNIL dispose du pouvoir de prononcer des amendes administratives, en fixe les plafonds et opère un renvoi à l'article 83 du RGPD pour connaître les critères à prendre en compte dans la détermination du montant de ces amendes. Ainsi, contrairement à ce que semble soutenir la société, ce n'est pas l'article 83 du RGPD qui est en l'espèce mis en application pour permettre à la formation restreinte de prononcer une amende, mais bien l'article 20 de la loi du 6 janvier 1978, dont l'application est expressément prévue par l'alinéa 6 de l'article L. 34-5 du CPCE et qui, lui, opère un renvoi aux critères de l'article 83 du RGPD pour la détermination du montant de l'amende.

Au regard des dispositions précitées, la formation restreinte considère donc qu'elle dispose du pouvoir de prononcer une amende pour un manquement à l'article L. 34-5 du CPCE.

En deuxième lieu, la société soutient que le rapport de sanction ne contient aucune motivation au regard des critères légaux justifiant le prononcé d'une amende et son montant. La société ajoute que l'amende proposée est disproportionnée au regard du contexte économique causé par la crise sanitaire de la Covid-19. Elle souligne que sa situation financière est déjà durement impactée par cette crise de sorte que le prononcé d'une amende à son encontre compromettrait sérieusement la pérennité de ses activités. La société produit à ce titre une attestation comptable certifiant que la trésorerie disponible estimée pour le mois de décembre 2020 s'élèverait à […] euros.

La formation restreinte considère au contraire que le prononcé d'une amende administrative est justifié au regard des critères posés par l'article 83 paragraphe 2 du RGPD.

S'agissant du manquement à l'article L. 34-5 du RGPD, la formation restreinte considère que la société a fait preuve d'une négligence grave en considérant qu'elle pouvait, pour constituer sa base de prospects, s'abstenir de recueillir le consentement des personnes. La gravité de cette violation est avérée en raison notamment du nombre particulièrement important de personnes concernées par le manquement et par le fait que la CNIL a été saisie de plusieurs plaintes, à l'origine de la procédure de contrôle de la CNIL.

S'agissant du manquement à l'obligation d'informer les personnes, la formation restreinte rappelle que l'information et la transparence relative au traitement des données à caractère personnel sont des obligations essentielles pesant sur les responsables de traitement afin que les personnes soient pleinement conscientes de l'utilisation qui sera faite de leurs données à caractère personnel, une fois celles-ci collectées.

Dès lors, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements aux articles L. 34-5 du CPCE et 12 et 13 du RGPD.

S'agissant du manquement à l'obligation de respecter le droit d'accès des personnes, en application de l'article 15 du RGPD, la formation restreinte relève que, dans le cadre de la procédure, la société a fait valoir qu'elle n'avait pas compris le périmètre des demandes et que les deux plaintes reçues ne démontrent pas un caractère structurel du manquement reproché à la société. S'agissant du manquement à l'obligation d'assurer la sécurité des données, en application de l'article 32 du RGPD, la formation restreinte considère qu'au vu des mesures prises par la société elle a fait preuve de bonne foi dans le cadre de la procédure. En conséquence, la formation restreinte considère, au regard des circonstances de l'espèce, qu'il n'y a pas lieu d'assoir son amende sur le fondement de ces deux manquements, bien qu'ils soient caractérisés.

S'agissant du montant de l'amende administrative, la formation restreinte rappelle que le paragraphe 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où il est reproché à la société un manquement aux articles L. 34-5 du CPCE et 12 et 13 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Toutefois, la formation restreinte tient également compte, dans la détermination du montant de l'amende prononcée, de la situation financière de la société. La société a fait état de son chiffre d'affaires estimé pour l'année 2020, pour la période du 1er janvier au 31 juillet, à […] euros, soit en forte baisse par rapport à 2019 où son chiffre d'affaire avait atteint […] euros au 31 décembre. La société fait également état d'une estimation pour la période du 1er janvier au 31 juillet 2020, de son résultat avant intérêts, impôts et amortissements, négatif de […] euros.

Dès lors, au regard du contexte économique causé par la crise sanitaire de la Covid-19, de ses conséquences sur la situation financière de la société et des critères pertinents de l'article 83, paragraphe 2, du Règlement évoqués ci-avant, la formation restreinte considère que le prononcé d'une amende de 20 000 euros apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83, paragraphe 1, de ce Règlement.

En troisième lieu, une injonction de mettre en conformité le traitement avec les dispositions des articles L. 34-5 du CPCE, 12, 13, 15 et 32 du RGPD a été proposée par le rapporteur lors de la notification du rapport.

S'agissant du manquement relatif à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un système automatisé de communications électroniques en application de l'article L. 34-5 du CPCE, la formation restreinte considère que la société ayant pris les mesures satisfaisantes pour recueillir le consentement des personnes lors de la création d'un compte sur l'application et sur le site web, et s'étant engagée, dans le cadre de la procédure, à ne plus procéder à l'envoi de messages de prospection directe par courriers électroniques à des prospects sans leur consentement préalable, l'injonction proposée dans le rapport n'est plus nécessaire. Cependant, la formation restreinte considère que la société n'a pas démontré avoir procédé à la suppression de la base de données des prospects dont le consentement préalable, libre, spécifique et informé à recevoir des messages de prospection directe par courriers électroniques n'a pas été recueilli par la société. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une injonction sur ce point.

S'agissant du manquement à l'obligation de respecter le droit d'accès des personnes, en application de l'article 15 du RGPD, la société soutient avoir mis en place une procédure interne permettant de faire droit aux demandes formulées au regard de l'article 15 du RGPD et l'avoir amendée afin de répondre aux demandes de droit d'accès de manière satisfaisante. Elle a communiqué sa procédure interne à la formation restreinte, conformément à l'invitation de cette dernière, le 6 novembre 2020.

La formation restreinte considère cependant que la société n'a pas pleinement répondu aux demandes de droit d'accès présentées par Monsieur X et Monsieur Y.

Ainsi, sans ignorer les démarches de la société pour se mettre en conformité avec le RGPD et la mise en place et l'amendement de sa procédure interne, la formation restreinte considère que la société n'a toujours pas démontré, sa conformité à l'article 15 du Règlement, faute d'avoir satisfait aux demandes de Monsieur X et de Monsieur Y. La formation restreinte considère en conséquence qu'il y a lieu de prononcer une injonction.

En quatrième lieu, la formation restreinte considère que la publicité de la sanction se justifie au regard de la pluralité des manquements relevés, de leur persistance et de leur gravité. En effet, la formation restreinte considère que, si la société a pris des mesures dans le cadre de la procédure de sanction permettant de mettre en conformité le traitement des données à caractère personnel qu'elle effectue, elle n'a cependant pas pris en compte l'ensemble des exigences fixées par l'article L. 34-5 du CPCE en matière de recueil du consentement, ni celles résultant de la loi Informatique et Libertés .

En outre, la formation restreinte considère que les pratiques de la société, qui a effectué des opérations de prospection par courriers électroniques en l'absence de contentement des personnes, justifient la publication de sa décision.

Enfin, la formation restreinte considère que la publication permettrait de renforcer le caractère dissuasif de la sanction principale.

PAR CES MOTIFS

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

- **prononcer à l'encontre de la société NESTOR SAS une amende administrative d'un montant de 20 000 (vingt mille) euros** pour les manquements aux articles L. 34-5 du Code des postes et des communications électroniques (ci-après le CPCE) et 12 et 13 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le RGPD),;

- **prononcer à l'encontre de la société NESTOR SAS une injonction de mettre en conformité les traitements** avec les obligations résultant des articles L. 34-5 du CPCE et 15 du RGPD, et en particulier :

• s'agissant du manquement à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un système automatisé de communications électroniques :

*Justifier de la suppression de l'ensemble des données à caractère personnel antérieurement collectées sans le consentement des prospects ;

•s'agissant du manquement à l'obligation de respecter le droit d'accès :

*Satisfaire pleinement aux demandes de droits d'accès en communiquant copie de l'ensemble de leurs données à caractère personnel détenues aux demandeurs, ainsi que le cas échéant, les informations relatives à la source d'où proviennent leurs données ;

-assortir l'injonction d'une astreinte de 500 (cinq cents) euros par jour de retard à l'issue d'un délai de 3 (trois) mois suivant la notification de la présente délibération, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai ;

- rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

Le Vice-Président

Philippe-Pierre CABOURDIN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.