Conseil d'État, 10ème chambre, 26/04/2022, 449284, Inédit au recueil Lebon

Conseil d'État - 10ème chambre

Audience publique du mardi 26 avril 2022

ECLI:FR:CECHS:2022:449284.20220426
Non publié au bulletin

Rapporteur
Mme Myriam Benlolo Carabot

Avocat(s)
SCP GADIOU, CHEVALLIER

Texte intégral

RÉPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête sommaire, un mémoire complémentaire et deux mémoires en réplique, enregistrés les 1er février, 30 avril, 5 août et 6 octobre 2021 au secrétariat du contentieux du Conseil d'Etat, la société Optical Center demande au Conseil d'Etat :

1°) d'annuler la délibération n° SAN-2021-001 par laquelle la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL) a prononcé à son encontre une amende administrative de 250 000 euros et lui a enjoint de mettre ses traitements de données à caractère personnel en conformité avec les articles 12 § 2 et 32 du règlement général sur la protection des données (RGPD), sous astreinte de 500 euros par jour de retard à l'issue d'un délai de trois mois suivant la notification de sa délibération, et d'enjoindre à la CNIL de prononcer la clôture de la procédure ;

2°) à titre subsidiaire, de réduire le montant de la sanction pécuniaire qui lui a été infligée ;

3°) à titre infiniment subsidiaire, de surseoir à statuer et de saisir la Cour de justice de l'Union européenne des deux questions préjudicielles suivantes :

" 1° Le droit de l'Union européenne, et plus particulièrement l' article 47 de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à ce que, par une décision d'une autorité nationale de contrôle des données personnelles, une entreprise ressortissante de l'Union européenne se soit vue privée d'un procès équitable, en ce que cette autorité s'est basée sur un rapport établi par une personne qu'elle a désignée, laquelle a manqué à ses devoirs d'impartialité et d'indépendance, avec pour conséquence que cette entreprise s'est vue infliger une lourde sanction financière malgré le fait qu'elle a activement collaboré à la mise en conformité de la situation en respectant les articles 32 et 33 du règlement général sur la protection des données ' ;

2° Le droit de l'Union européenne, et plus particulièrement les articles 49 de la Charte des droits fondamentaux et 83 du RGPD, qui garantissent le respect de la règle de proportionnalité des peines, doivent-ils être interprétés en ce sens qu'ils s'opposent à une décision nationale prononçant une peine financière très lourde, laquelle est intervenue sans respecter la gradation des peines prévues par le RGPD et sans avoir mis l'entreprise en demeure au préalable, et cela malgré le fait que cette dernière a respecté les articles 32 et 33 du RGPD, qu'aucune personne concernée n'a subi de dommages et que la mise en conformité des traitements litigieux a été assurée par l'entreprise sanctionnée dans les meilleurs délais ' ".

4°) de mettre à la charge de la Commission nationale de l'informatique et des libertés la somme de 6 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu les autres pièces du dossier ;

Vu :
- la Charte des droits fondamentaux de l'Union européenne ;
- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;
- la loi n° 78-17 du 6 janvier 1978 ;
- le décret n° 2019-536 du 29 mai 2019 ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de Mme Myriam Benlolo Carabot, maître des requêtes en service extraordinaire,

- les conclusions de M. Laurent Domingo, rapporteur public ;

La parole ayant été donnée, après les conclusions, à la SCP Gadiou, Chevallier, avocat de la société Optical Center ;

Vu la note en délibéré, enregistrée le 21 avril 2022, présentée pour la société Optical Center.

Considérant ce qui suit :

1. Il résulte de l'instruction qu'à la suite de la notification faite, le 4 janvier 2019, par la société Optical Center à la Commission nationale de l'informatique et des libertés (CNIL) d'une attaque sur son site internet de vente en ligne ainsi qu'au dépôt de plusieurs plaintes de clients et de prospects de cette société, la CNIL a procédé, les 19 février, 29 avril et 27 et 28 mai 2019, à plusieurs contrôles, sur place dans les locaux de la société et en ligne sur son site web, pour vérifier la conformité de ses traitements de données à caractère personnel avec les dispositions du règlement général sur la protection des données (RGPD) du 27 avril 2016 et de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Par une délibération en date du 6 janvier 2021, la formation restreinte de la CNIL a prononcé à l'encontre de la société Optical Center une amende administrative d'un montant de 250 000 euros à raison des manquements constatés aux dispositions des articles 12 paragraphe 2 et 32 du RGPD et lui a enjoint de mettre ses traitements en conformité avec ces dispositions, sous astreinte de 500 euros par jour de retard à l'issue d'un délai de trois mois suivant la notification de sa délibération.

Sur la régularité de la procédure devant la CNIL :

2. En premier lieu, l'article 22 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que les sanctions infligées par la formation restreinte de la CNIL " sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable de traitement ou à son sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. (...) ". Alors même que le rapporteur n'a pas voix délibérative, le moyen tiré de la méconnaissance du principe d'impartialité par le rapporteur est de nature, s'il s'avère fondé, à entraîner l'annulation de la sanction prononcée par la formation restreinte de la CNIL. Toutefois, il résulte de l'instruction que ni les prises de position politiques exprimées par M. Pellegrini, rapporteur désigné par la CNIL, sur son compte Facebook, librement accessible, ni le fait qu'il ait déjà été désigné comme rapporteur d'une précédente procédure de sanction contre la société Optical Center, ne révèlent, dans les circonstances de l'espèce, un parti pris défavorable à cette dernière. Il s'ensuit que la société requérante n'est pas fondée à soutenir que la procédure suivie à son encontre aurait méconnu le principe d'impartialité ainsi que son droit à un procès équitable garanti par l'article 47 de la Charte des droits fondamentaux faute pour la CNIL d'avoir fait droit à sa demande de récusation du rapporteur.

3. En second lieu, conformément au III de l'article 20 de la loi du 6 janvier 1978, dans sa rédaction issue de l'ordonnance du 12 décembre 2018 : " 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 après avoir prononcé à son encontre une ou plusieurs des mesures correctrices prévues au II, saisir la formation restreinte de la commission " en vue du prononcé, après procédure contradictoire, d'une ou plusieurs mesures de sanction. Il résulte des termes mêmes de ces dispositions que le prononcé d'une sanction par la formation restreinte de la CNIL n'est pas subordonné à l'intervention préalable d'une mise en demeure du responsable du traitement ou de son sous-traitant par le

président de la CNIL. Il s'ensuit que le moyen tiré de ce que la présidente de la CNIL aurait méconnu les dispositions du III de l'article 20 de la loi du 6 janvier 1978 en saisissant la formation restreinte sans adresser à la société requérante une mise en demeure préalable, ne peut qu'être écarté alors même que la société Optical Center avait elle-même informé la CNIL de l'attaque informatique dont elle avait fait l'objet et avait commencé à prendre des mesures correctrices. Par ailleurs, dès lors que la possibilité de prononcer une mise en demeure est prise en compte pour apprécier la proportionnalité de la sanction, le moyen tiré de ce que l'absence de mise en demeure méconnaîtrait le principe de proportionnalité des peines garanti par l'article 49 de la Charte des droits fondamentaux ne peut qu'être écarté.

Sur les manquements :

4. En premier lieu, conformément à l'article 32 du règlement général sur la protection des données du 27 avril 2016, il incombe au responsable de traitement et au sous-traitant de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, et notamment, en fonction des risques que présente le traitement, des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement, ainsi que de mettre en place une procédure permettant de tester, analyser et évaluer régulièrement l'efficacité de ces mesures.

5. Il résulte de l'instruction, d'une part, que la vulnérabilité du système informatique à l'origine de la violation des données de près de 200 000 clients européens est la conséquence directe de l'absence de mise en œuvre par la société Optical Center d'un contrôle régulier sur les mesures techniques et organisationnelles prises par son sous-traitant chargé d'assurer la sécurité de son site web, aucun document produit par cette dernière ne permettant de justifier de la mise à jour régulière des différents composants logiciels du site. D'autre part, le manque de robustesse de la politique de mots de passe de la société eu égard aux catégories de données traitées qui incluent notamment le numéro de sécurité sociale de ses clients, a accru l'exposition de son système à un risque d'attaque informatique. Par suite, les moyens tirés de ce que la formation restreinte de la CNIL aurait méconnu les dispositions de l'article 32 du règlement précité et commis une erreur d'appréciation en considérant qu'elle avait manqué aux obligations en découlant, ne peuvent qu'être écartés.

6. En second lieu, conformément au paragraphe 2 de l'article 12 du règlement général sur la protection des données du 27 avril 2016, le responsable de traitement facilite l'exercice des droits conférés à la personne concernée en vertu des articles 15 à 22 du même règlement, en particulier de son droit d'accès aux données traitées ainsi que de son droit de s'opposer à tout moment au traitement de ses données à des fins de prospection.

7. Il résulte de l'instruction, d'une part, que les adresses électroniques communiquées sur le site web de la société et destinées à recueillir les demandes relatives à l'exercice des droits conférés à la personne, prévus par les articles 15 à 22 du règlement général sur la protection des données, étaient erronées. Ce dysfonctionnement n'a été pleinement réparé qu'à l'issue d'un délai de plus de six mois, et postérieurement au contrôle diligenté par les services de la CNIL. D'autre part, la procédure d'exercice de ces mêmes droits dans le cadre des opérations de prospection commerciale effectuées par voie postale par un prestataire de la société Optical Center ne permettait pas de faciliter les démarches des personnes concernées, en l'absence de transmission directe des demandes de droit d'accès du responsable de traitement à son prestataire. Il s'ensuit que la formation restreinte de la CNIL n'a pas méconnu les dispositions de l'article 12 du RGPD et n'a entaché sa délibération d'aucune erreur d'appréciation en retenant que la société avait méconnu ses obligations en matière d'exercice des droits des personnes dont les données sont traitées, le nombre de plaintes instruites par la CNIL au regard du volume de demandes reçues à ce titre par la société étant sans incidence sur la portée du manquement constaté.

Sur le montant de la sanction infligée :

8. D'une part, conformément au 7° du III de l'article 20 de la loi du 6 janvier 1978, en cas de non-respect par le responsable de traitement ou son sous-traitant des obligations résultant de la loi ou du RGPD, la formation restreinte de la CNIL peut infliger " 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 ".

9. D'autre part, en vertu de l'article 83 du RGPD, les amendes administratives imposées par les autorités de contrôle nationales doivent, dans chaque cas, être " effectives, proportionnées et dissuasives ". Pour fixer le montant de l'amende, doivent, notamment, être pris en considération : " a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ; / b) le fait que la violation a été commise délibérément ou par négligence ; / c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ; / d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ; / e) toute violation pertinente

commise précédemment par le responsable du traitement ou le sous-traitant ; / f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ; / g) les catégories de données à caractère personnel concernées par la violation ; / h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ; / i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ; / j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et / k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation ".

10. Il résulte de l'instruction que pour fixer à 250 000 euros le montant de l'amende administrative infligée à la société Optical Center à raison des manquements aux articles 12, paragraphe 2, et 32 du RGPD, la formation restreinte de la CNIL a retenu que, si la société n'avait pas commis intentionnellement les manquements reprochés et avait activement coopéré avec ses services, elle a néanmoins méconnu deux obligations élémentaires en matière de sécurité informatique et a fait preuve d'une négligence durable s'agissant de la protection des droits des personnes. Elle a observé que ces manquements se sont traduits par la violation des données à caractère personnel de plus de 200 000 personnes et le dysfonctionnement du dispositif permettant l'exercice du droit d'accès de plusieurs centaines de milliers de prospects ou clients, et que les catégories de données qui ont fait l'objet de l'attaque informatique révèlent des informations personnelles telles que les nom, prénom, adresse, numéro de téléphone, adresse électronique, date de naissance, et, pour 23 000 d'entre elles, le numéro de sécurité sociale. Elle a enfin rappelé que la société avait été sanctionnée à deux reprises au cours des cinq dernières années pour des manquements à la sécurité des données à caractère personnel et un manquement lié à la sous-traitance de ses traitements de données. Compte tenu de l'ensemble de ces éléments et eu égard au chiffre d'affaires de 202 millions d'euros réalisé par la société au titre de l'année 2017, la formation restreinte de la CNIL n'a pas, en retenant un montant de 250 000 euros, infligé une amende disproportionnée à la société Optical Center.

11. Il résulte de tout ce qui précède, sans qu'il soit besoin, en l'absence de tout doute raisonnable quant à la portée des articles 47 et 49 de la Charte des droits fondamentaux de l'Union européenne et de l'article 83 du règlement général sur la protection des données, ainsi qu'il ressort des points 2 et 3 de la présente décision, de saisir la Cour de justice de l'Union européenne de questions préjudicielles, que la société requérante n'est pas fondée à demander l'annulation de la délibération de la formation restreinte de la CNIL qu'elle attaque. Ses conclusions au titre de l'article L. 761-1 du code de justice administrative ne peuvent, par suite, qu'être rejetées.

D E C I D E :

Article 1er : La requête de la société Optical Center est rejetée.
Article 2 : La présente décision sera notifiée à la société Optical Center et à la Commission nationale de l'informatique et des libertés.

Délibéré à l'issue de la séance du 17 mars 2022 où siégeaient : M. Bertrand Dacosta, président de chambre, présidant ; M. Alexandre Lallet, conseiller d'Etat et Mme Myriam Benlolo Carabot, maître des requêtes en service extraordinaire-rapporteure.

Rendu le 26 avril 2022.

Le président :
Signé : M. Bertrand Dacosta

La rapporteure :
Signé : Mme Myriam Benlolo Carabot

La secrétaire :
Signé : Mme A... B...

ECLI:FR:CECHS:2022:449284.20220426