



Délibération SAN-2023-003 du 16 mars 2023

Commission Nationale de l'Informatique et des Libertés Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mardi 28 mars 2023

Délibération de la formation restreinte n° SAN-2023-003 du 16 mars 2023 concernant la société CITYSCOOT

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Christine MAUGÜÉ, Madame Anne DEBET, Monsieur Bertrand du MARAIS et Monsieur Alain DRU, membres ;

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, notamment ses articles 56 et 60 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés notamment ses articles 20 et suivants ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2020-081C du 12 mai 2020 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 de tout traitement accessible à partir du domaine " cityscoot.eu " et l'application mobile " CITYSCOOT " ;

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 12 avril 2021 ;

Vu le rapport de Madame Valérie PEUGEOT, commissaire rapporteure, notifié à la société CITYSCOOT le 17 mars 2022 ;

Vu les observations écrites versées par la société CITYSCOOT le 2 mai 2022 ;

Vu la réponse de la rapporteure notifiée à la société le 16 juin 2022 ;

Vu les observations écrites versées par la société CITYSCOOT le 29 juillet 2022, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Etaient présents, lors de la séance de la formation restreinte du 29 septembre 2022 :

- Madame Valérie Peugeot, commissaire, entendue en son rapport ;

En qualité de représentants de la société CITYSCOOT :

[...]

La société CITYSCOOT ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société CITYSCOOT (ci-après " la société ") est une société par actions simplifiée au capital de 121 002,10 euros, sise 8 rue Bayen à Paris (75017), créée en 2014. La société estime ses effectifs en France à 225 personnes. Elle a réalisé, en 2019, un chiffre d'affaires de 21 882 031 euros pour un résultat net déficitaire de 12 641 302 euros. Dans un courrier du 21 avril 2021, la société a estimé son chiffre d'affaires pour l'exercice clos au 31 décembre 2020 à un montant de [...].

2. Depuis 2016, la société propose un service de location de scooters électriques en libre-service accessible à partir de l'application mobile " CITYSCOOT ". Il s'agit d'une offre de véhicules partagés en " freefloating ", c'est-à-dire qui se caractérise par l'absence de stations. Les scooters ne sont pas stationnés dans des espaces précis et peuvent être laissés, après utilisation, dans la zone de location identifiée dans l'application. Les scooters sont équipés d'un dispositif de

localisation embarquée qui permet à CITYSCOOT et aux utilisateurs, via leur application mobile, de connaître la position des scooters. La location d'un scooter électrique auprès de la société suppose la création d'un compte à partir de l'application mobile. Il s'agit d'un service sans engagement qui est facturé à la minute.

3. En France, ce service est disponible en région parisienne et à Nice. Par ailleurs, la société a également développé son service dans certaines villes d'Italie et d'Espagne par l'intermédiaire de deux filiales qu'elle détient à 100%, CITYSCOOT ITALIA S.R.L. et CITYSCOOT ESPANA SL. La société dénombre à ce jour environ 247 000 utilisateurs en France et à l'étranger.

4. Un contrôle en ligne a été effectué sur le site web " cityscoot.eu " et l'application mobile " CITYSCOOT ", le 13 mai 2020. Le procès-verbal n°2020-081/1, dressé par la délégation le jour du contrôle, a été notifié à la société le 19 mai 2020. La délégation de la CNIL s'est notamment attachée à vérifier les données collectées et les finalités de la collecte. Ce contrôle avait également pour but de vérifier l'encadrement de la sous-traitance et la sécurité des données.

5. Trois demandes de complément d'informations ont ensuite été adressées à la société par une lettre recommandée avec avis de réception du 26 juin 2020 et par courriers électroniques des 27 août et 10 décembre 2020. La société a répondu à ces demandes par des courriers datés des 16 juillet, 11 septembre et 15 décembre 2020.

6. Conformément à l'article 56 du RGPD, la CNIL a informé l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier mis en œuvre par CITYSCOOT, à savoir la gestion des comptes utilisateurs et des outils mis en place par la société, résultant de ce que l'établissement principal de la société se trouve en France. Après échange entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, l'Espagne et l'Italie se sont déclarées concernées par ledit traitement.

7. Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné Madame Valérie PEUGEOT en qualité de rapporteure, le 12 avril 2021, sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

8. Le 17 février 2022, la rapporteure a fait parvenir à la société une demande complémentaire relative à l'anonymisation des données à caractère personnel effectuée par un hachage des données et de l'application d'un sel. La société y a répondu par un courrier du 23 février 2022.

9. La rapporteure a fait notifier à la société CITYSCOOT, le 17 mars 2022, un rapport détaillant les manquements aux 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 Informatique et Libertés " ou " loi du 6 janvier 1978 modifiée ") qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer à l'encontre de la société une amende administrative et de rendre la décision publique mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

10. Le 2 mai 2022, la société a produit ses observations en réponse au rapport de sanction.

11. Par un courrier du 16 juin 2022, la réponse de la rapporteure a été adressée à la société.

12. Le 29 juillet 2022, la société a adressé de nouvelles observations en réponse à celles de la rapporteure.

13. Par un courrier du 22 août 2022, la rapporteure a informé la société de la clôture de l'instruction.

14. Le 23 août 2022, le président de la formation restreinte a notifié à la société CITYSCOOT une convocation pour la séance du 29 septembre 2022.

II. Motifs de la décision

15. En application de l'article 60, paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 15 février 2023 aux autorités de contrôle européennes concernées.

16. Au 15 mars 2023, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

A. Sur le manquement relatif à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données à caractère personnel traitées en application de l'article 5, paragraphe 1, c) du RGPD

17. L'article 5, paragraphe 1, c) du RGPD prévoit que les données à caractère personnel doivent être " adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ". Lorsque les données sont collectées sur le fondement de l'intérêt légitime, cette collecte ne doit en outre pas porter une atteinte disproportionnée à la vie privée, au regard des objectifs poursuivis par la société.

18. La rapporteure relève que, dans le cadre de l'instruction, la délégation de contrôle de la CNIL a été informée que les scooters sont équipés de boîtiers électroniques comprenant une carte SIM et un système de géolocalisation GPS, embarqués sur les scooters. Ces boîtiers collectent des données de position des scooters toutes les 30 secondes lorsque le CITYSCOOT est actif et que son tableau de bord est allumé, qu'il soit en déplacement ou prêt à rouler. Lorsque le CITYSCOOT est inactif, le boîtier collecte des données de position toutes les 15 minutes.

19. Ces données sont stockées dans " une base de données scooters " qui contient notamment les données suivantes : la position via le GPS et " un numéro de réservation [...] qui sont collectés dans le cas où le Cityscoot est réservé, durant la période de location ". Elles sont conservées 12 mois en base active, puis 12 mois en archivage intermédiaire avant d'être anonymisées.

20. Les données de position des scooters, à savoir la localisation du scooter au point de départ et d'arrivée de la réservation et la localisation pendant tout le trajet sont collectées par la société pour les finalités suivantes : traitement des infractions au code de la route, traitement des réclamations clients, support aux utilisateurs (afin d'appeler les secours en cas de chute d'un utilisateur), gestion des sinistres et des vols.

21. Pour mettre fin à la location, l'utilisateur doit effectuer certaines manipulations telles que : s'assurer d'être dans une zone autorisée pour garer les scooters (zone CITYSCOOT), éteindre le scooter, presser le bouton " FIN " situé sur le scooter ou cliquer sur " TERMINER MA LOCATION " dans l'application mobile et vérifier que la diode verte " LIBRE " est allumée.

22. La rapporteure considère qu'aucune des finalités avancées par la société ne justifie une collecte quasi permanente des données de géolocalisation au cours de la location d'un scooter.

23. Il y a lieu d'examiner la pertinence de la collecte de ces données pour chacune de ces finalités. A titre liminaire, la formation restreinte souligne que, dès lors qu'un véhicule est en cours de location, les données de géolocalisation issues de ce véhicule sont associées à une personne et constituent des données à caractère personnel. En revanche, lorsque le scooter n'est pas loué, les données de géolocalisation liées au seul véhicule ne sont pas des données à caractère personnel.

24. La formation restreinte note que la société utilise trois bases de données distinctes :

- une " base de données scooter " qui contient les données remontées par les capteurs fixés sur le scooter (position du scooter via un GPS, état de la batterie, capteur de la selle) ;

- une " base de données réservation " qui contient les dates et heures de début et de fin de chaque location ainsi que l'état du scooter au début et à la fin de sa location ;

- une " base de données client " qui comprend les données permettant de gérer la facturation, cette dernière base ne contenant pas de données relatives au scooter.

25. La formation restreinte relève que, si les données de position des scooters sont décorrélées de toute information relatives aux utilisateurs dans la " base de données scooter " et sont conservées dans une base distincte de celle stockant les données relatives aux utilisateurs, à savoir la " base de données client ", ce qui constitue un choix d'architecture informatique respectueux de la vie privée (privacy by design), il n'en demeure pas moins que ces données peuvent être recoupées avec les données présentes dans les autres bases, notamment par le biais du numéro de réservation présent dans chacune des bases, en disposant d'un accès étendu et simultané aux bases de données.

26. La formation restreinte considère donc que les données de géolocalisation collectées par CITYSCOOT lorsque le scooter est en cours de location, sont des données à caractère personnel dès lors qu'un rapprochement est possible entre les différentes bases de données, quand bien même ce rapprochement ne serait que ponctuel, les données de position de scooter se rapportant à une personne physique identifiée ou identifiable.

27. En outre, la formation restreinte relève que, si les données de géolocalisation ne sont pas des données sensibles, au sens de l'article 9 du RGPD, elles sont néanmoins considérées par le groupe de travail de l'article 29 (dit " G29 " devenu le Comité européen de la protection des données (CEPD)) dans ses lignes directrices du 4 octobre 2017, comme étant des " données à caractère hautement personnel ". Le CEPD estime que ces données sont considérées comme sensibles, au sens commun du terme, dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental : la collecte des données de localisation met en jeu la liberté de circulation.

28. A titre d'éclairage, la formation restreinte rappelle également que le CEPD a considéré, dans ses lignes directrices 01/2020 relatives aux traitements de données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité (les lignes directrices 01/2020) que " lorsqu'ils collectent des données à caractère personnel, les constructeurs de véhicules et d'équipements, les prestataires de services et les autres responsables du traitement devraient garder à l'esprit que les données de localisation sont particulièrement révélatrices des habitudes de vie des personnes concernées. Les trajets réalisés sont très caractéristiques en ce qu'ils peuvent permettre de déduire le lieu de travail, le domicile ainsi que les centres d'intérêt (loisirs) du conducteur, et peuvent éventuellement révéler des informations sensibles comme la religion, par l'intermédiaire du lieu de culte, ou l'orientation sexuelle, par l'intermédiaire des lieux fréquentés. Par conséquent, les constructeurs de véhicules et d'équipements, les prestataires de services et les autres responsables du traitement devraient particulièrement veiller à ne pas collecter de données de localisation, à moins que cela ne soit absolument nécessaire pour la finalité du traitement ". Ces lignes directrices soulignent également que la collecte de données de localisation est subordonnée au respect du principe selon lequel la localisation peut être activée " uniquement lorsque l'utilisateur lance une fonctionnalité qui nécessite de connaître la localisation du véhicule, et non par défaut et en continu au démarrage de la voiture ".

29. Bien que la société conteste l'applicabilité des lignes directrices au cas d'espèce, au motif qu'elles ne concerneraient que les automobiles, la formation restreinte considère que les lignes directrices constituent un éclairage pertinent s'agissant des données de géolocalisation en général.

30. Dans ce cadre, la formation restreinte rappelle que l'appréciation du respect du principe de minimisation des données repose sur le caractère limité à ce qui est nécessaire des données traitées au regard de la finalité pour laquelle elles sont collectées. Son appréciation implique de procéder à une analyse de nécessité des données à caractère personnel qui sont collectées au regard des finalités visées.

31. Au regard des éléments qui précèdent, la formation restreinte considère qu'il convient d'analyser uniquement la nécessité de la collecte et de la conservation des données de position collectées toutes les 30 secondes, dès lors que la collecte des données de position au début et à la fin de location est pertinente au regard des finalités poursuivies.

32. En premier lieu, s'agissant de la gestion des réclamations liées à la surfacturation, la rapporteure considère que la collecte des données de géolocalisation toutes les trente secondes pendant toute la durée de la location n'est pas nécessaire. Elle précise que la gestion de la surfacturation devrait être gérée par la prise de contact de l'utilisateur lorsqu'il rencontre une difficulté à mettre fin à sa location ou, à tout le moins, par des moyens moins intrusifs qu'une géolocalisation quasi-permanente du véhicule en cours de location.

33. En défense, la société fait valoir que la collecte des données de position des scooters toutes les 30 secondes serait nécessaire, dans le cadre d'un service facturé à la minute pour des situations ayant engendré une surfacturation et une réclamation de la part des utilisateurs lorsqu'ils n'ont pas réussi à mettre fin correctement à leur location, notamment lorsque :

- l'utilisateur perd la communication avec un scooter pour des raisons techniques ou humaines ;
- l'utilisateur fait une réclamation liée aux zones de stationnement non autorisées ;
- l'utilisateur n'arrête pas le scooter correctement pour mettre fin à la location ;
- le scooter a été déplacé par un tiers.

34. La collecte des données de position toutes les 30 secondes permettrait de remonter par tranches de 30 secondes pour identifier le nombre de secondes pendant lequel le scooter a été à l'arrêt. Elle ajoute que les utilisateurs se rendent compte, très souvent a posteriori, que la location n'a pas été correctement terminée et ne prennent pas attache avec la société au moment de mettre fin à la location. Le déclenchement de la géolocalisation au moment de la prise de contact par l'utilisateur ne suffirait donc pas car il ne serait pas possible de calculer les minutes surfacturées entre le moment où l'utilisateur a souhaité mettre fin à la location et n'a pas pu le faire, et le moment où la société a pu régler le problème et mettre fin à la location.

35. La formation restreinte prend note des arguments mis en avant par la société pour gérer les réclamations liées à la surfacturation. Elle relève cependant que, à cette fin, la collecte et la conservation des données de géolocalisation des scooters toutes les 30 secondes n'est pas nécessaire.

36. En effet, dans trois des cas évoqués par la société (perte de communication avec le scooter, difficulté liée aux zones non autorisées, scooter déplacé par un tiers), la formation restreinte considère que l'utilisateur peut prendre attache avec la société CITYSCOOT pour résoudre les difficultés et terminer la location. La géolocalisation pourrait donc être déclenchée à compter de ce fait générateur.

37. En ce qui concerne les cas où l'utilisateur n'arrête pas le scooter correctement pour mettre fin à la location, la formation restreinte souligne que la géolocalisation du scooter toutes les 30 secondes ne permet pas de déterminer à quel moment l'utilisateur souhaitait réellement mettre fin à sa location. En effet, la position statique du scooter, à elle seule, ne démontre pas la volonté de l'utilisateur de ne pas poursuivre sa location.

38. En outre, la formation restreinte précise qu'il serait possible de mettre en place des mécanismes alternatifs et moins intrusifs permettant à la société de s'assurer que l'utilisateur a bien mis fin à la location ou, au contraire, de l'avertir lorsque ce n'est pas le cas, par exemple par l'envoi d'un SMS ou la confirmation, par une alerte via l'application, que la location a pris fin.

39. Si la société affirme avoir reçu, pour le mois de juin 2022, environ 11 500 appels sur 386 766 courses relatifs à des problèmes de surfacturation, elle n'indique pas la part des appels liés à ce cas spécifique. La formation restreinte considère, à défaut de statistiques précises, que ces cas ne sauraient justifier la géolocalisation quasi-permanente de tous les scooters.

40. Au demeurant, la formation restreinte remarque que l'article 7.4.6 des conditions générales d'utilisation de CITYSCOOT prévoit qu'" il est de la responsabilité de l'utilisateur de contrôler que la fin de sa Location est effective. CITYSCOOT ne pourra être tenue responsable d'une facturation prolongée en cas de mauvaise restitution du Scooter ". Il revient donc à l'utilisateur de s'assurer qu'il a correctement mis fin à la location.

41. En deuxième lieu, s'agissant de la gestion des amendes, la rapporteure considère que les données de géolocalisation des scooters tout au long du trajet ne sont pas nécessaires pour identifier l'utilisateur responsable de l'infraction dès lors qu'un recoupement entre le moment de l'infraction et la personne ayant loué le scooter sur cette période suffit pour le faire.

42. En défense, la société affirme que la collecte de la position des scooters toutes les 30 secondes est nécessaire pour obtenir des informations sur les circonstances et le contexte d'une infraction. L'objectif est de vérifier si l'infraction relevée par l'ANTAI (" Agence nationale de traitement automatisé des infractions ") a bien été commise : confirmer ou infirmer la présence du scooter à l'endroit relevé par l'avis de contravention et vérifier si l'infraction a pu se produire à cet endroit. Elle considère également que la collecte des données de position des scooters est nécessaire pour pouvoir identifier ou prouver l'identité du conducteur auprès de l'ANTAI, de la police ou des compagnies d'assurance.

43. La formation restreinte considère, d'une part, qu'il n'est pas nécessaire pour la société de collecter et conserver la position des scooters toutes les 30 secondes pour identifier et prouver l'identité d'un conducteur auprès de l'ANTAI, de la police ou des compagnies d'assurance. En effet, la collecte du numéro et la date de l'avis de contravention, la date et l'heure du début et de la fin de la location, la date et l'heure de l'infraction suffisent pour répondre à cette finalité. Ces données croisées avec le numéro de plaque d'immatriculation du scooter permettent en effet d'identifier la personne ayant loué le scooter. Au demeurant, la collecte des données de position des scooters ne permet pas d'établir en tant que telle l'identité de la personne responsable de l'infraction dès lors qu'il n'est pas possible de déterminer si le scooter a été déplacé par la personne ayant loué le scooter ou s'il a été déplacé par une tierce personne sur une mauvaise zone de stationnement, étant donné que le scooter peut être librement déplacé avec ou sans le moteur en marche.

44. D'autre part, la formation restreinte considère que la collecte et la conservation des données de position des scooters, toutes les 30 secondes, est excessive dans la mesure où elle concerne la totalité des scooters loués par la société alors qu'elle ne répond qu'à une finalité incidente dans le cas où un utilisateur aurait besoin de ces données pour contester une infraction au code de la route.

45. En troisième lieu, s'agissant de la gestion des vols, la rapporteure souligne que, pour être considéré comme proportionné, le traitement de données de géolocalisation doit être rendu nécessaire à cette finalité par un fait générateur, tel qu'une déclaration de vol ou une suspicion de vol. Les données de géolocalisation des scooters ne peuvent donc pas être considérées comme nécessaires à la poursuite de la finalité liée au risque de vol, avant tout fait générateur.

46. En défense, la société affirme que la collecte des données de scooter en cas de vol ne signifie pas pour autant que ces données sont croisées avec l'identité des utilisateurs. Elle ajoute qu'elle a besoin des données de position des scooters uniquement pour localiser ses scooters afin de les retrouver et les récupérer en cas de vol.

47. La société précise qu'elle ne peut se reposer uniquement sur les indications de la dernière position fournie par l'utilisateur au moment de la déclaration de vol, qui ne sont pas nécessairement fiables et que certaines difficultés techniques (batterie vidée, problème technique ou encore lorsque le scooter se trouve dans un parking ou une zone dans laquelle la géolocalisation ne peut pas être déclenchée) peuvent l'empêcher de déclencher la géolocalisation à distance. Elle précise également que la collecte des données de position des scooters toutes les 30 secondes permet de réduire considérablement la zone de recherche en cas de vol et que le système de géolocalisation, qui est intégré au scooter, ne peut pas être désactivé par une personne cherchant à voler le scooter.

48. La formation restreinte rappelle avant tout que, quand bien même la société ne procéderait pas à un rapprochement entre les données de position des scooters et les données de l'utilisateur pour retrouver un véhicule volé, la possibilité de faire ce rapprochement entre les différentes bases de données justifie que les données de position des scooters soient considérées comme des données à caractère personnel, soumises aux exigences du RGPD.

49. Par ailleurs, comme le relève la rapporteure, avant tout fait générateur, les données de géolocalisation des scooters ne peuvent pas, en principe, être considérées comme nécessaires à la poursuite de cette finalité et leur collecte en permanence ou de manière très rapprochée doit être considérée comme excessive.

50. A titre d'éclairage, la formation restreinte relève que les lignes directrices 01/2020 du CEPD indiquent que les données de localisation ne peuvent être remontées qu'à partir de la déclaration de vol et ne sauraient être collectées en continu le reste du temps. A cet égard, le CEPD recommande également que le responsable de traitement informe clairement la personne concernée qu'il n'existe pas de traçage permanent du véhicule et que les données de géolocalisation ne peuvent être collectées et transmises qu'à partir de la déclaration de vol.

51. En outre, la formation restreinte souligne que l'appréciation du caractère limité à ce qui est nécessaire, au sens de l'article 5, paragraphe 1, c) du RGPD, est éclairée par les dispositions du considérant 39 du RGPD, selon lequel " les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens ". L'existence de moyens moins intrusifs pour atteindre les mêmes finalités doit être ainsi prise en compte, qu'il s'agisse de moyens alternatifs ou de données traitées moins fréquemment ou en moins grand nombre.

52. Avant tout, la formation restreinte précise que si le scooter est volé en dehors d'une période de location, les données de position du scooter ne sont pas rattachées à une réservation et ne permettent donc pas d'identifier un individu. Ce ne sont alors pas des données à caractère personnel et une telle situation est donc en dehors du champ de la présente procédure.

53. La formation restreinte estime ensuite qu'aucun scénario de vol ne justifie une collecte des données de position toutes les 30 secondes. D'une part, les cas, dont la société n'a pas établi la fréquence, où le scooter est volé en cours d'utilisation, c'est-à-dire lorsque l'utilisateur est lui-même sur le scooter en marche, ne doivent pas justifier la collecte quasi-permanente des données de position du scooter. D'autre part, le scooter peut être volé lorsque l'utilisateur fait une pause dans le cadre de sa location. Dans ce cas, l'utilisateur pourra contacter immédiatement la société CITYSCOOT dès le constat du vol en fin de pause, ce qui renseignera la société sur la dernière position du scooter.

54. Interrogée sur le nombre de véhicules retrouvés grâce à la dernière position connue du scooter, la société n'a pas été en mesure de fournir des statistiques démontrant l'efficacité de la géolocalisation toutes les 30 secondes.

55. Ainsi, la formation restreinte souligne que, au regard des considérations qui précèdent, les cas où d'une part, la géolocalisation est le seul moyen de connaître la dernière position connue du scooter et où, d'autre part, cette dernière position connue est effectivement proche de la localisation du scooter, apparaissent limités. Dans ces situations, la formation restreinte ne remet pas en cause l'utilité de connaître la dernière position connue du scooter grâce à la dernière donnée de géolocalisation. Cependant, cette hypothèse ne suffit pas à justifier la collecte des données de géolocalisation toutes les 30 secondes de l'ensemble des trajets des utilisateurs.

56. Au regard de ces considérations, la formation restreinte estime que, dans une grande partie des cas d'usage, la collecte et conservation des données de géolocalisation toutes les 30 secondes au cours de la location du scooter n'est pas nécessaire à la gestion des vols. Le fait de procéder systématiquement à cette collecte, pour les cas d'usages où elle pourrait être effectivement utile sur le fondement de l'intérêt légitime de la société, apparaît porter une atteinte disproportionnée à la vie privée. En effet, comme cela a été souligné ci-dessus, la collecte et conservation par la société de l'ensemble des trajets des utilisateurs des scooters la conduisent à manipuler des données hautement personnelles (v. CNIL, FR, 7 juillet 2022, Sanction, n° SAN-2022-015, publié).

57. En quatrième lieu, s'agissant de la gestion des accidents, la rapporteure soutient que la collecte des données de géolocalisation à cette fin ne peut intervenir qu'à compter d'un fait générateur, notamment la notification technique lorsque le scooter est trop incliné ou une demande d'assistance par le client, rendant cette collecte nécessaire.

58. En défense, la société affirme qu'il est nécessaire de collecter les données de position des scooters toutes les 30 secondes et de les croiser avec les données des utilisateurs afin de pouvoir contacter l'utilisateur lorsque le détecteur a envoyé une notification technique révélatrice d'un accident et assister cet utilisateur dans le cadre de la déclaration et des démarches de constat. Elle ajoute que les accidents ne déclenchent pas nécessairement une notification technique, notamment lorsque le scooter ne s'incline pas suffisamment. Elle précise également qu'elle est régulièrement sollicitée par des sociétés d'assurance, a posteriori, pour obtenir des informations sur des accidents dont elle n'avait pas connaissance, comme la localisation précise du scooter au moment de l'accident.

59. La formation restreinte souligne d'abord qu'il est légitime pour la société de vouloir porter assistance aux utilisateurs victimes d'un accident de la circulation pendant la location d'un scooter. Cependant, pour porter une telle assistance aux utilisateurs, la société doit avoir connaissance de la survenance d'un accident.

60. La formation restreinte considère que, dès lors que la société a connaissance de la survenance d'un accident concernant un scooter loué, elle peut géolocaliser ce véhicule pour, le cas échéant, porter assistance à l'utilisateur.

61. La formation restreinte considère que, dans la grande majorité des cas, un fait générateur permet à la société d'avoir connaissance de l'accident, que ce soit la notification technique du scooter trop incliné ou l'appel de l'utilisateur.

62. La formation restreinte estime que la géolocalisation toutes les 30 secondes de l'ensemble des scooters au cours de toute la durée de location, préalablement à toute information relative à un accident, n'est pas nécessaire pour porter assistance à un utilisateur. La collecte et conservation des données de géolocalisation quasi-permanente n'est donc ni adéquate, ni pertinente au regard de cette finalité.

63. Il résulte de l'ensemble de ce qui précède que la formation restreinte considère qu'aucune des finalités avancées par la société ne justifie une collecte toutes les 30 secondes des données de géolocalisation au cours de la location d'un scooter et la conservation de ces données. Une telle pratique est en effet très intrusive dans la vie privée des utilisateurs dans la mesure où elle est susceptible de révéler leurs déplacements, leurs lieux de fréquentation, la totalité des arrêts effectués au cours d'un parcours, ce qui revient à mettre en cause leur liberté de circuler anonymement. La formation restreinte relève à cet égard qu'il ressort des développements supra que la société pourrait proposer un service identique sans collecter les données de géolocalisation de manière quasi-permanente.

64. La formation restreinte considère par conséquent que ces faits constituent un manquement à l'article 5, paragraphe 1, c) du RGPD.

B. Sur le manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel proportionnée à la finalité du traitement en application de l'article 5, paragraphe 1, e) du RGPD

65. Aux termes de l'article 5, paragraphe 1, e) du Règlement, les données à caractère personnel doivent être " conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) "

66. La rapporteure a relevé dans son rapport qu'il ressort des échanges avec la société que les données de position des scooters sont conservées sans limite de durée dans la base de données scooters alors que la société précise par ailleurs que ces données sont anonymisées au bout de vingt-quatre mois. La rapporteure a considéré que le fait de conserver les données de géolocalisation d'un utilisateur sans limite de durée ou pendant vingt-quatre mois en base active excède la durée nécessaire au regard des finalités pour lesquelles les données sont traitées, relatives à la gestion des réclamations des clients et la gestion des amendes, sinistres et vols.

67. En défense, la société a expliqué que, contrairement à ce qui était indiqué dans le rapport, elle ne conserve pas de données à caractère personnel " sans limite de durée " et en aucun cas pendant vingt-quatre mois en base active. Elle a précisé que les données de position des scooters sont conservées pendant douze mois en base active et que, à l'issue de ces douze mois, les données de position des scooters ne sont plus conservées en base active mais sont archivées dans une base intermédiaire. Après cette conservation de douze mois en archivage intermédiaire, les données font l'objet d'une anonymisation.

68. Lors de la séance, compte tenu des éléments communiqués par la société dans le cadre de l'instruction, la rapporteure a considéré que les durées et les modalités de conservation des données, au regard des finalités évoquées, sont conformes aux exigences du RGPD. Elle a, en conséquence, proposé à la formation restreinte de ne pas retenir le manquement en cause.

69. La formation restreinte considère que le manquement à l'article 5, paragraphe 1, e) du RGPD n'est pas constitué.

C. Sur le manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués par un sous-traitant en application de l'article 28, paragraphe 3 du RGPD

70. Aux termes de l'article 28, paragraphe 3 du RGPD, le traitement effectué par un sous-traitant pour un responsable de traitement doit être régi par un contrat qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées ainsi que les obligations et les droits du responsable de traitement. Ce contrat doit prévoir en outre les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement.

71. La rapporteure a pu constater que la société CITYSCOOT fait appel à quinze sous-traitants ayant un accès ou hébergeant des données à caractère personnel. Sur ces quinze contrats, elle considère que les contrats avec les sociétés

[...] ne contiennent pas toutes les mentions prévues par le RGPD. Le contrat avec la société [...] ne prévoit que de manière générale les obligations de sécurité qui incombent au sous-traitant et il n'évoque pas l'obligation du sous-traitant de mettre à disposition du responsable de traitement toutes les informations pour démontrer le respect des obligations prévues, permettre la réalisation d'audits et contribuer à ces audits. Le contrat avec la société [...] ne prévoit pas une procédure de suppression ou de renvoi des données à caractère personnel du sous-traitant au responsable de traitement à échéance du contrat. Le contrat avec la société [...], très lacunaire, ne prévoit pas notamment l'objet du traitement, ni sa durée. Enfin, le contrat avec la société [...] ne vise pas la catégorie de personnes concernées par le traitement.

72. En défense, la société affirme que les contrats avec les sociétés [...] ont été modifiés, à la suite des contrôles des services de la CNIL, afin de se mettre en conformité avec le RGPD. S'agissant du contrat avec la société [...], la société considère que le sous-traitant s'engage bien à mettre en œuvre les mesures qui sont celles requises par l'article 32 du RGPD et que le contrat prévoit les conditions dans lesquelles le sous-traitant met à la disposition de CITYSCOOT les informations nécessaires. S'agissant du contrat avec la société [...], la société affirme que les données sont traitées en conformité avec la politique du sous-traitant relative à la conservation des données selon laquelle toute donnée est supprimée ou effacée après la fin de la période de conservation, période qui est de 14 mois avant anonymisation.

73. La formation restreinte rappelle, à titre liminaire, que dans ses lignes directrices 07/2020 du 7 juillet 2021 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, le CEPD affirme que " tandis que les éléments visés à l'article 28 du règlement constituent le contenu essentiel du contrat, ce dernier devrait permettre au responsable du traitement et au sous-traitant de clarifier davantage la manière dont ces éléments essentiels seront mis en œuvre en recourant à des instructions détaillées. Par conséquent, l'accord de traitement ne devrait pas se contenter de reproduire les dispositions du RGPD ; il devrait inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord " (§ 112). Partant, les mentions visées à l'article 28, paragraphe 3 doivent non seulement figurer dans le contrat de sous-traitance, mais elles doivent également être suffisamment précises et détaillées pour permettre d'assurer un traitement conforme des données à caractère personnel.

74. S'agissant du contrat avec la société [...], la clause " accountability " prévoit effectivement que le sous-traitant doit répondre aux questions du responsable de traitement et lui fournir, sur demande, tout document sollicité. Cependant, il n'est pas indiqué expressément que le sous-traitant doit tenir à sa disposition toutes les informations pour permettre la réalisation d'audits et contribuer à ces audits.

75. La formation restreinte considère également que la clause " security ", qui prévoit que le sous-traitant met en place des mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque, devrait être plus précise. En effet, à titre d'illustration, dans ses lignes directrices 07/2020, le CEPD affirme que " l'accord devrait éviter de se contenter de répéter ces obligations d'assistance et devrait contenir des précisions sur la manière dont le sous-traitant est invité à aider le responsable du traitement à remplir les obligations énumérées. Par exemple, des procédures et des formulaires types peuvent être joints en annexes à l'accord pour permettre au sous-traitant de fournir au responsable du traitement toutes les informations nécessaires [...] le sous-traitant est d'abord tenu d'aider le responsable du traitement à respecter l'obligation d'adopter des mesures techniques et organisationnelles appropriées afin de garantir la sécurité du traitement. Bien que cela puisse, dans une certaine mesure, empiéter sur l'exigence selon laquelle le sous-traitant adopte lui-même des mesures de sécurité appropriées, lorsque les opérations de traitement du sous-traitant relèvent du champ d'application du RGPD, ces deux obligations demeurent distinctes, l'une se référant aux mesures propres au sous-traitant et l'autre à celles du responsable du traitement ". Ici, seuls les objectifs de sécurité à atteindre sont décrits, sans précision sur les moyens d'y parvenir, tels qu'une description des processus ou mécanismes développés dans des annexes au contrat. En l'absence de précision sur les moyens pour remplir l'obligation de mettre en place des mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque, la formation restreinte considère que le contrat ne répond pas aux exigences du RGPD.

76. S'agissant du contrat avec la société [...], la formation restreinte considère que si le contrat prévoit une politique de durée de conservation des données à caractère personnel, il n'est pas fait mention du sort des données en cas de résiliation du contrat entre les deux sociétés. En effet, la politique de durée de conservation des données et le sort des données à l'échéance du contrat font l'objet de deux mentions différentes par l'article 28, paragraphe 3 du RGPD. L'article 28, paragraphe 3, (g) prévoit que le contrat doit indiquer que le sous-traitant " selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes ". Dès lors, cette mention doit donc être visée spécifiquement et séparément dans le contrat.

77. S'agissant des contrats avec les sociétés [...], la formation restreinte prend acte du fait que la société s'est assurée de mettre les contrats en conformité avec les exigences du RGPD. Cependant, à la date des contrôles, lesdits contrats ne répondaient pas à ces exigences. En effet, le contrat avec la société [...], très lacunaire, ne visait notamment pas l'objet du traitement, la durée du traitement, le type de données à caractère personnel traité. Le contrat conclu avec la société [...], quant à lui, ne précisait pas la catégorie de personnes visées par le traitement.

78. Dès lors, au regard de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 28 paragraphe 3 du RGPD est caractérisé.

D. Sur le manquement à l'obligation d'informer l'utilisateur et d'obtenir son consentement avant d'inscrire et de lire des informations sur son équipement terminal de communication électronique en application de l'article 82 de la loi du 6 janvier 1978

79. L'article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée dispose que " tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant : 1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ; 2° Des moyens dont il dispose pour s'y opposer. Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne

utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle. Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur : 1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; 2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ".

80. La rapporteure considère que la société CITYSCOOT, en tant qu'elle édite le site web " cityscoot.eu " et l'application mobile CITYSCOOT, a une part de responsabilité dans le respect des obligations de l'article 82 de la loi " Informatiques et Libertés " pour les opérations de lecture et / ou d'écriture d'informations effectuées dans le terminal des utilisateurs via le mécanisme de reCaptcha fourni par la société Google, lors de la création du compte sur l'application mobile ainsi que lors de la connexion et la procédure de mot de passe oublié sur le site internet. La rapporteure a constaté que la société CITYSCOOT ne fournit aucune information, notamment par une fenêtre de consentement, de la collecte d'informations stockées sur l'équipement de l'utilisateur, ni des moyens de refuser cette collecte. Le consentement de l'utilisateur portant sur l'accès aux informations stockées sur son équipement ou sur l'inscription d'informations sur son équipement n'est recueilli à aucun moment.

81. En défense, la société affirme utiliser le mécanisme de reCaptcha dans le seul but d'assurer la sécurisation du mécanisme d'authentification des utilisateurs. Elle précise que la mise en place d'un tel mécanisme est conforme à la délibération n° 2017-012 du 19 janvier 2017 de la CNIL laquelle ne précise pas qu'il est obligatoire de recueillir le consentement des utilisateurs. Elle ajoute que l'utilisation de reCaptcha doit bénéficier de la seconde exemption prévue à l'article 82 de la loi " Informatique et Libertés " en ce que le service est demandé par l'utilisateur - à savoir l'inscription ou la connexion au service de CITYSCOOT - et que les actions de lecture et d'écriture des informations présentes sur les terminaux sont nécessaires pour assurer la sécurité du service. Elle précise que si elle n'est pas tenue de recueillir le consentement de ses utilisateurs pour l'utilisation qu'elle fait elle-même du reCaptcha, elle ne saurait être tenue de le recueillir pour le compte de la société Google. Elle affirme que le mécanisme de reCaptcha Google, directement intégré sur le site, prévoit un lien qui renvoie à la politique de confidentialité de Google, laissant sous-entendre que la société Google se considère comme responsable du traitement et informe elle-même les utilisateurs. Par ailleurs, la société CITYSCOOT ne peut pas modifier elle-même la présentation ou le paramétrage du mécanisme et n'a donc pas la faculté d'intégrer une case à cocher ou un autre lien d'information. La société affirme que la délibération n° 2020-092 du 17 septembre 2020 est postérieure à la procédure de contrôle et ne peut être appliquée pour l'analyse de recueil de consentement des utilisateurs, l'analyse devant être effectuée sur le régime antérieur à ladite délibération. Elle conclut toutefois qu'elle n'aura plus recours à ce mécanisme à compter d'octobre 2022.

82. La formation restreinte relève, en premier lieu, que le Conseil d'Etat a jugé (CE, 6 juin 2018, Editions Croque Futur, n° 412589, Rec.), qu'au titre des obligations qui pèsent sur l'éditeur d'un site qui dépose des " cookies tiers ", figurent celle de s'assurer auprès de ses partenaires, d'une part, qu'ils n'émettent pas, par l'intermédiaire de son site, des traceurs qui ne respectent pas la réglementation applicable en France, et d'autre part, celle d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements. Le Conseil d'Etat a en particulier jugé que " les éditeurs de site qui autorisent le dépôt et l'utilisation de tels " cookies " par des tiers à l'occasion de la visite de leur site doivent également être considérés comme responsables de traitement, alors même qu'ils ne sont pas soumis à l'ensemble des obligations qui s'imposent au tiers qui a émis le " cookie ", notamment lorsque ce dernier conserve seul la maîtrise du respect de sa finalité ou de sa durée de conservation. Au titre des obligations qui pèsent sur l'éditeur de site dans une telle hypothèse, figurent celle de s'assurer auprès de ses partenaires qu'ils n'émettent pas, par l'intermédiaire de son site, des " cookies " qui ne respectent pas la réglementation applicable en France et celle d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements " (v. également CNIL, FR, 27 septembre 2021, Sanction, n° SAN-2021-013, publié).

83. La formation restreinte relève en outre que si les recommandations émises par la Commission en matière de cookies ont évolué récemment pour tenir compte des évolutions induites par le RGPD en matière de consentement notamment, ces évolutions n'ont pas d'incidence dans le cas d'espèce et il a continuellement été considéré, comme l'indique la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978 depuis abrogée, que " lorsque plusieurs acteurs interviennent dans le dépôt et la lecture de cookies (par exemple lorsque les éditeurs facilitent le dépôt de cookies qui sont ensuite lus par des régies publicitaires), chacun d'entre eux doit être considéré comme coresponsable des obligations découlant des dispositions de l'article 32-II précité [actuel article 82 de la loi du 6 janvier 1978] ". Cette délibération précise qu'il en est ainsi " des éditeurs de sites internet (ou des éditeurs d'application mobile par exemple) et de leurs partenaires (régies publicitaires, réseaux sociaux, éditeurs de solutions de mesure d'audience...). En effet, dans la mesure où les éditeurs de site constituent souvent l'unique point de contact des internautes et que le dépôt de Cookies de tiers est tributaire de la navigation sur leur site, il leur appartient de procéder, seuls ou conjointement avec leurs partenaires, à l'information préalable et au recueil du consentement explicités à l'article 2 de la présente recommandation ". La formation restreinte précise d'ailleurs qu'elle a déjà consacré la responsabilité des éditeurs de sites internet dans plusieurs décisions (v. en ce sens, Délibération SAN-2021-013 du 27 juillet 2021).

84. La formation restreinte constate qu'un mécanisme de reCaptcha, fourni par la société Google, est utilisé lors de la création du compte sur l'application mobile ainsi que lors de la connexion et la procédure de mot de passe oublié sur le site internet. La formation restreinte considère que c'est bien l'éditeur du site – en l'espèce CITYSCOOT - qui a choisi de recourir au mécanisme de reCaptcha et a donc permis les actions de lecture et d'écriture des informations présentes sur les terminaux des utilisateurs.

85. Au regard des éléments qui précèdent, la formation restreinte considère que la société n'est pas fondée à soutenir qu'aucune obligation ni aucune responsabilité ne lui incombent quant aux opérations effectuées par Google via le reCaptcha tendant à accéder à des informations déjà stockées dans l'équipement terminal de communications électroniques des utilisateurs, ou à inscrire des informations dans cet équipement, sans leur consentement, lorsqu'ils visitent son site. Elle considère donc que la société est également responsable du respect des dispositions de l'article 82 de la loi " Informatique et libertés " lors de l'utilisation du mécanisme de reCaptcha de Google.

86. En deuxième lieu, la formation restreinte considère que si un responsable de traitement peut se prévaloir d'une exemption à l'information et au recueil du consentement lorsque les opérations de lecture/écriture effectuées dans le terminal d'un utilisateur ont pour seule finalité la sécurisation d'un mécanisme d'authentification au bénéfice des utilisateurs (v. en ce sens, CNIL, FR, 27 septembre 2021, Sanction, n° SAN-2021-013, publié), il en va autrement lorsque ces opérations poursuivent également d'autres finalités qui ne sont pas strictement nécessaires à la fourniture d'un service. Or, le mécanisme de reCaptcha Google n'a pas pour seule finalité la sécurisation du mécanisme d'authentification au bénéfice des utilisateurs mais permet par ailleurs des opérations d'analyse de la part de Google, ce que la société Google précise elle-même dans ses conditions générales d'utilisation.

87. La formation restreinte relève que la société GOOGLE informe les sociétés ayant recours à la technologie reCaptcha, dans des conditions générales d'utilisation disponibles en ligne, que le fonctionnement de l'API reCAPTCHA repose sur la collecte d'informations matérielles et logicielles (telles que les données sur les appareils et les applications) et que ces données sont transmises à Google pour analyse. La société GOOGLE précise également qu'il incombe à ces sociétés d'informer les utilisateurs et de demander leur autorisation pour la collecte et le partage des données avec GOOGLE.

88. En l'espèce, il ressort de ces éléments que la société CITYSCOOT aurait dû informer les utilisateurs et recueillir leur consentement, ce qui n'est pas le cas en l'espèce.

89. En effet, si la société CITYSCOOT informait, à la date du contrôle, les utilisateurs, dans le cadre de sa politique de confidentialité, que " lors de votre visite sur notre Site ou Application, des données de navigation et de localisation, issues des cookies ou des technologies similaires, seront collectées ", les finalités précises des cookies utilisés, la possibilité de s'y opposer ou le fait que la poursuite de la visite constituait une forme de consentement ne figuraient pas parmi les informations fournies par la société. En outre, l'information, accessible via la politique de confidentialité sur le site, n'était fournie que postérieurement au dépôt de cookies et autres traceurs et de manière non spécifique alors que la recommandation issue de la délibération n° 2020-092 du 17 septembre 2020 prévoit clairement que l'information doit être spécifique et antérieure au dépôt. Partant, il ne peut être considéré que les utilisateurs étaient informés et que le consentement était valablement recueilli à l'aune des recommandations de la délibération n° 2020-092 du 17 septembre 2020.

90. En dernier lieu, s'agissant de l'opposabilité de la délibération n° 2020-092 du 17 septembre 2020 aux fins d'analyse du recueil du consentement des utilisateurs, la formation restreinte rappelle que la délibération n° 2020-092 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux " cookies et autres traceurs " vise à interpréter les dispositions législatives applicables et à éclairer les acteurs sur la mise en place de mesures concrètes permettant de garantir le respect de ces dispositions, afin qu'ils mettent en œuvre ces mesures ou des mesures d'effet équivalent. En ce sens, il est précisé dans les recommandations que celles-ci " ont pour objet principal de rappeler et d'explicitier le droit applicable aux opérations de lecture et/ou d'écriture d'informations (ci-après les " traceurs ") dans l'équipement terminal de communications électroniques de l'abonné ou de l'utilisateur (ci-après " utilisateurs ")".

91. La Commission a rappelé, dans le cadre de sa recommandation du 17 septembre 2020, que " lorsqu'aucune des exceptions prévues à l'article 82 de la loi " Informatique et Libertés " n'est applicable, les utilisateurs doivent, d'une part, recevoir une information conforme à cet article, complétée, le cas échéant, par les exigences du RGPD, et, d'autre part, se voir indiquer les conséquences de leur choix ".

92. La formation restreinte relève que la CNIL n'a pas créé dans sa recommandation de nouvelles obligations à la charge des acteurs mais s'est bornée à illustrer concrètement comment l'article 82 de la loi doit trouver à s'appliquer.

93. A cet égard, la circonstance que la recommandation du 17 septembre 2020 ne serait pas opposable à la société compte tenu des modalités de recueil du consentement applicables à la date du contrôle, est sans incidence dès lors que l'article 82 de la loi Informatique et libertés prévoit que " tout utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant : 1. De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ; 2. Des moyens dont il dispose pour s'y opposer ".

94. En tout état de cause, la formation restreinte relève que la société n'a pas informé l'utilisateur, et cela même au regard des dispositions de l'ancienne recommandation issue de la délibération n° 2013-378 du 5 décembre 2013, antérieure à celles de la délibération n° 2020-092, de la finalité précise des cookies, de la possibilité de s'y opposer et du fait que la poursuite de la navigation vaut accord au dépôt de cookies sur son terminal.

95. Enfin, la formation restreinte prend note que la société CITYSCOOT entend ne plus avoir recours à ce mécanisme à compter d'octobre 2022. Cependant, à la date des contrôles, ledit mécanisme était bien utilisé.

96. Dès lors, au vu de ce qui précède, la formation restreinte considère que la société a méconnu ses obligations au regard de l'article 82 de la loi " Informatique et Libertés " en permettant le dépôt de cookies sur le terminal des utilisateurs via le mécanisme de reCaptcha fourni par la société Google sans informer les utilisateurs et sans recueillir leur consentement.

III. Sur les mesures correctrices et la publicité

97. 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 : [...]

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 ".

98. 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 ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

99. En premier lieu, s'agissant du principe du prononcé d'une amende, la formation restreinte rappelle qu'elle doit tenir compte, pour le prononcé d'une amende administrative, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

100. La formation restreinte considère d'abord que la société a fait preuve de défaillances graves en matière de protection des données à caractère personnel puisque des manquements à des principes fondamentaux et élémentaires du RGPD et de la loi " Informatique et Libertés " sont constitués, tels que les principes de minimisation des données et le recueil du consentement des utilisateurs avant d'inscrire et de lire des informations sur son équipement terminal de communication électronique.

101. La formation restreinte relève ensuite que l'atteinte aux droits des personnes qui résulte du manquement au principe de minimisation des données à caractère personnel est particulièrement importante, au regard de la nature particulière des données de géolocalisation. En effet, la société procède à une collecte quasi permanente de données de géolocalisation des utilisateurs des scooters qu'elle loue. Une telle collecte est particulièrement intrusive pour les utilisateurs. En effet, elle permet de suivre l'ensemble des trajets réalisés par l'utilisateur, d'identifier les lieux où il se rend, pouvant révéler ainsi des informations sur son comportement, ses habitudes de vie, ce qui est susceptible de porter atteinte à sa vie privée et à sa liberté de circuler anonymement.

102. La formation restreinte souligne également que les données à caractère personnel traitées par la société concernent environ 247 000 utilisateurs, répartis sur le territoire de trois États membres de l'Union européenne.

103. La formation restreinte relève également que certains contrats conclus par la société CITYSCOOT avec ses sous-traitants sont incomplets et ne contiennent pas toutes les mentions prévues par l'article 28, paragraphe 3 du RGPD ou ne prévoient pas de manière assez précise les obligations qui incombent au sous-traitant.

104. S'agissant du mécanisme de reCaptcha, la formation restreinte considère que le manquement relatif à l'article 82 de la loi " Informatique et Libertés " est caractérisé par le fait que la société n'a pas respecté les exigences en matière d'information et de recueil du consentement, ce qui a eu pour effet de priver les utilisateurs du choix qu'ils doivent pouvoir exprimer quant aux modalités selon lesquelles leurs données personnelles seront utilisées.

105. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements constitués aux articles 5, paragraphe 1, c) et 28, paragraphe 3 du RGPD et à l'article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

106. En deuxième lieu, s'agissant du montant de l'amende, la formation restreinte rappelle que les amendes administratives doivent être effectives, proportionnées et dissuasives.

107. En l'espèce, la société a méconnu ses obligations au titre des articles 5, paragraphe 1, c) et 28, paragraphe 3 du RGPD et de l'article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée à l'égard d'environ 247 000 utilisateurs.

108. La formation restreinte prend toutefois en compte le fait que, à l'issue des contrôles effectués par la délégation de la CNIL, la société s'est mise en conformité sur les contrats conclus avec les sociétés [...] au regard des exigences de l'article 28, paragraphe 3 du RGPD.

109. Elle rappelle également que l'activité de l'organisme et sa situation financière doivent être prises en compte pour la détermination de la sanction et notamment, en cas d'amende administrative, de son montant. Elle relève à ce titre que la société a réalisé, en 2019, un chiffre d'affaires de 21 882 031 euros, pour un résultat net en perte, de -12 641 302 euros. La société a estimé son chiffre d'affaires pour l'exercice clos au 31 décembre 2020 à un montant de [...].

110. Dès lors, au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende administrative de 100 000 euros au titre des manquements au RGPD et 25 000 euros au titre du manquement à la loi " Informatique et Libertés " apparaît justifié.

111. En troisième lieu, la formation restreinte considère que la publicité de la sanction se justifie au regard de la nature particulière des données concernées qui portent sur des données de géolocalisation et de l'atteinte à la vie privée des utilisateurs.

PAR CES MOTIFS

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

- prononcer à l'encontre de la société CITYSCOOT une amende administrative d'un montant de 100 000 (cent mille) euros au regard des manquements constitués aux articles 5, paragraphe 1, c) et 28, paragraphe 3 du 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 et 25 000 (vingt-cinq mille) euros au regard du manquement constitué à l'article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée ;

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

Le président

Alexandre LINDEN

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.