Date de publication sur legifrance: 19/07/2018

Commission Nationale de l'Informatique et des Libertés

Décision n°MED-2018-022 du 25 juin 2018
Décision n° MED 2018-022 du 25 juin 2018 mettant en demeure la société TEEMO

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée par 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 le code pénal ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 45 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié 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° 2017-108C du 12 avril 2017 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 auprès de la société DATABERRIES ;

Vu la décision n° 2017-216C du 29 septembre 2017 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 auprès de la société DATABERRIES ;

Vu les procès-verbaux de contrôle n° 2017-108/1 du 7 juin 2017 et n° 2017-216/1 du 2 octobre 2017 ;

Vu les autres pièces du dossier ;

La société TEEMO (ci-après la société), sise 39, rue Godot de Mauroy à Paris (75009) est une société anonyme spécialisée dans l'édition de logiciels applicatifs. Elle emploie environ 35 salariés et a réalisé en 2016, un chiffre d'affaires d'environ 2,4 millions d'euros.

L'ancien nom commercial de la société est DATABERRIES ; elle est désormais

enregistrée au greffe du Tribunal de commerce sous le nom TEEMO.

L'activité de la société TEEMO est d'afficher des publicités interstitielles[1]pour le compte de ses partenaires, sur les ordiphones de personnes dont le profil est sélectionné à partir de leurs données de géolocalisation. La société a également pour activité de mesurer les visites des mobinautes[2]dans les points de vente physiques de ses partenaires.

La société a effectué, le 7 juillet 2015, auprès de la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) une déclaration n° 1873686 relative au traitement de données de géolocalisation à des fins d'amélioration des applications mobiles et à des fins de marketing.
La société a désigné, le 28 mars 2018, un Délégué à la protection des données .
En application des décisions n° 2017-108C du 12 avril 2017 et 2017-216C du 29 septembre 2017 de la Présidente de la Commission, une délégation de la CNIL a procédé les 7 juin et 2 octobre 2017 à des missions de contrôle sur place auprès de la société TEEMO. Les missions ont notamment eu pour objet de vérifier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée) de l'ensemble des traitements de données à caractère personnel mis en œuvre par la société.
La société TEEMO conclut des contrats avec des sociétés, essentiellement des enseignes de magasin telles que […], […] ou […]. Elle détermine avec ses partenaires des points d'intérêts (ci-après POIs) qui correspondent à des coordonnées géographiques, tels que des points de vente physiques. L'objectif de la société TEEMO est d'établir des profils des mobinautes afin de leur proposer de la publicité ciblée. Sont ainsi, par exemple, ciblés les mobinautes s'étant rendus dans des magasins concurrents et ceux ayant visité le magasin d'un partenaire au cours des 30 derniers jours. Par la suite, la société TEEMO réalise des campagnes marketing à travers l'achat d'espaces publicitaires pour le compte de ses annonceurs partenaires, sur les plateformes de ventes aux enchères de publicités en temps réels.

La société TEEMO a développé un traceur SDK [3]permettant de collecter les données de géolocalisation des mobinautes ainsi que l'identifiant publicitaire mobile de leur smartphone.

Dans un premier temps, le SDK est intégré dans le code des applications mobiles de sociétés partenaires de la société TEEMO, tels que […] ou […], et permet de collecter les données en arrière-plan du fonctionnement des applications installées par les utilisateurs sur leurs smartphones.

Dans un second temps, les données de géolocalisation collectées grâce au SDK sont croisées avec les POIs déterminés par les partenaires de la société TEEMO, ce qui permet de qualifier le profil de l'utilisateur. Ces données sont conservées au sein de la base de données Matcher2 par la société TEEMO.

Lors du contrôle, la délégation a été informée que le SDK collecte les données de géolocalisation des personnes environ toutes les cinq minutes. La délégation a constaté que, sur une journée, 1 635 402 identifiants publicitaires associés à des données de géolocalisation avaient été collectées par la société. Chacun de ces identifiants publicitaires est directement lié au smartphone d'une personne ayant téléchargé l'application d'un de ses partenaires.

La délégation a également constaté qu'étaient présents dans la base de données, 13 977

539 d'identifiants publicitaires distincts collectés sur les treize derniers mois, correspondant à autant de smartphones de personnes physiques.

Par ailleurs, la délégation a constaté, sur plusieurs applications mobiles contrôlées intégrant le SDK de la société TEEMO, que lorsque l'utilisateur d'un smartphone valide l'autorisation d'accès à ses données de géolocalisation pour le fonctionnement de l'application, ses données sont également transmises à la société TEEMO sans qu'il en soit informé et sans que son consentement ne soit recueilli pour cette transmission.

En outre, la délégation a été informée que toutes les données de géolocalisation des mobinautes sont collectées et conservées sur les serveurs de la société, même lorsqu'ils sont situés en dehors des points d'intérêts géographiques déterminés par ses partenaires.

La délégation a constaté que les données de géolocalisation des personnes, collectées à partir des applications mobiles des partenaires, sont conservées pendant treize mois à compter de la date de la collecte.

Enfin, la délégation a constaté que le contrat conclu entre la société et la société Google pour l'hébergement des bases de données ne prévoit pas de clauses relatives à la sécurité et à la confidentialité des données.

À la suite de demandes formulées par la délégation, la société a apporté des éléments additionnels, par courriel du 17 novembre 2017, concernant notamment l'information des mobinautes et les modalités de recueil de leur consentement.

· Sur la notion de responsable du traitement et de données à caractère personnel

Sur la qualité de responsable du traitement

Aux termes de l'article 3-I de la loi du 6 janvier 1978 modifiée *le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens .*

Au regard des constats effectués par la CNIL et des pièces fournies lors des différents contrôles, il apparaît que la société TEEMO détermine dans une large mesure les finalités et les moyens des traitements mis en œuvre dans le cadre de l'utilisation du SDK.

En effet, la délégation a notamment constaté que les données des utilisateurs des applications mobiles sont intégrées et mutualisées au sein de la base de données Matcher2 de la société TEEMO. La délégation a également été informée que la société TEEMO traite pour son propre compte les données à caractère personnel collectées par le SDK installé au sein des applications de ses partenaires. Il lui a en effet été précisé que les données de géolocalisation collectées par le SDK sont analysées et interprétées par TEEMO pour en déduire des audiences qualifiées.

La société TEEMO doit, par conséquent, être considérée comme responsable du traitement mis en œuvre dans le cadre de l'utilisation du SDK.

Sur la collecte de données à caractère personnel

Aux termes de l'article 2 de la loi du 6 janvier 1978 modifiée constitue une donnée à caractère personnel *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne .*

Constitue en outre un traitement de données à caractère personnel *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction .*
La délégation a constaté que la société TEEMO collecte, *via* le SDK installé au sein des applications mobiles, l'identifiant publicitaire du smartphone associé à des données de géolocalisation de la personne ainsi qu'à des données techniques relatives au smartphone.

L'identifiant publicitaire est un identifiant unique généré par le système d'exploitation du smartphone permettant d'identifier le terminal de l'utilisateur de façon stable dans le temps. Il est mis à disposition de l'ensemble des applications mobiles installées sur celui-ci et est également accessible aux différents SDK installés dans les applications mobiles.

Cet identifiant publicitaire est stocké de façon pérenne dans le smartphone de l'utilisateur et permet donc d'identifier l'utilisateur de façon indirecte. Il a vocation à identifier l'utilisateur afin de lui associer un profil publicitaire constitué à partir de ses données de géolocalisation. Il permet donc d'identifier l'utilisateur lors de son utilisation ultérieure d'autres applications mobiles sur son téléphone afin de lui associer son profil publicitaire et de lui afficher des publicités spécifiquement choisies en fonction de ses habitudes de déplacement.

Il en résulte que la société traite des données à caractère personnel en application de l'article 2 de la loi du 6 janvier 1978 modifiée.

· <u>Sur les manquements constatés au regard des dispositions de la loi du 6 janvier 1978</u>

Un manquement à l'obligation de disposer d'une base légale pour la mise en œuvre du traitement

La délégation a été informée que la société procède à la collecte des données de géolocalisation des personnes à l'aide du traceur SDK intégré dans les applications mobiles téléchargées par les mobinautes. Par la suite, les données de géolocalisation sont croisées avec les points d'intérêts afin de qualifier le profil des personnes et de procéder à des opérations de démarchage publicitaire auprès d'elles.

Or, une telle combinaison des données à caractère personnel des mobinautes, à des fins publicitaires, ne peut intervenir que si la société peut se prévaloir de l'une des conditions prévues à l'article 7 de la loi n° 78-17 du 6 janvier 1978 modifiée, qui prévoit que :

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;
2° La sauvegarde de la vie de la personne concernée ;
3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le traitement des données de géolocalisation aux fins de marketing ciblé est, selon son responsable la société TEEMO, fondé sur le consentement des personnes concernées. En effet, la société a déclaré à la CNIL, lors du contrôle du 7 juin 2017 et dans son courriel du 17 novembre suivant, qu'il est prévu dans les contrats passés avec ses éditeurs d'applications mobiles partenaires que ces derniers sont tenus d'obtenir le consentement préalable des utilisateurs à l'accès aux données de géolocalisation stockées sur leur smartphone.

En vertu de l'article 2, point h) de la directive, le consentement s'entend comme *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement .*

À cet égard, la notion de consentement, reprise dans le règlement général sur la protection des données, n'est pas moins exigeante dès lors qu'il est prévu que celui-ci doit être donné *par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant .*

Or, il ressort des contrôles et de l'analyse des pièces transmises à la Commission qu'aucun mécanisme n'est proposé aux utilisateurs ayant téléchargé les applications des partenaires de la société pour consentir préalablement aux traitements opérés par cette dernière.

En premier lieu, le consentement doit être informé.

Le groupe de travail de l'article 29 (G29), dans son avis 15/2011 du 13 juillet 2011 sur la définition du consentement, a indiqué que *Ceci implique que toutes les informations nécessaires doivent être données au moment de la demande du consentement et que ces informations doivent couvrir tous les aspects de fond du traitement que le consentement est censé légitimer .*

En l'espèce, la délégation a constaté qu'au moment de l'installation des applications contrôlées, les personnes ne sont pas informées de la collecte de leurs données de géolocalisation *via* le SDK à des fins de profilage des utilisateurs et de ciblage publicitaire.

La société a informé la CNIL, par courrier électronique du 17 novembre 2017, qu'elle oblige contractuellement les partenaires à *informer explicitement leurs utilisateurs sur le fait que des données de géolocalisation sont utilisées à des fins de marketing et partagées avec des tiers .*

La société indique recommander également à ses partenaires, dans ses contrats,

d'insérer une bannière d'information sur l'application, lors de la première connexion des utilisateurs, comportant la mention suivante : *Dans l'application nous collectons des données relatives à votre expérience, votre navigation et votre géolocalisation. Ces données nous permettent d'optimiser votre expérience utilisateur, d'analyser notre trafic et de vous proposer des contenus plus pertinents. Certaines informations sont partagées avec nos partenaires. En poursuivant votre navigation dans l'application, vous acceptez la collecte de ces données .* La société précise que *Cette bannière serait par ailleurs associée à une case à cocher (ou un j'accepte) qui fermerait alors la fenêtre de la bannière* .

La société s'est également engagée à ce que la charte vie privée de ses partenaires indique explicitement que les données de géolocalisation sont collectées à des fins marketing et partagées avec des tiers.

La seule recommandation de la société TEEMO effectuée auprès de ses partenaires, relative à la mise en place d'une bannière lors de la première connexion des utilisateurs, ne permet pas d'assurer une information systématique des personnes de la collecte de leurs données de géolocalisation à des fins de publicité ciblée.

Il apparaît, en outre, que l'information délivrée au sein des chartes vie privée des applications mobiles est tardive dès lors qu'elle n'est accessible aux personnes qu'après l'installation de l'application et du SDK, alors que leur identifiant publicitaire et leurs données de localisation sont déjà collectées par la société TEEMO *via* le SDK.

Au surplus, la délégation a été informée, lors du contrôle du 2 octobre 2017, que lorsqu'un nouveau partenariat est conclu avec une société, le SDK est intégré au smartphone du mobinaute à l'occasion d'une mise à jour de l'application si celle-ci est déjà téléchargée. Or, à cette occasion les nouvelles conditions générales d'utilisation ou politiques de vie privée des applications ne sont pas directement portées à la connaissance des mobinautes.

Dès lors, les personnes ayant téléchargé l'application mobile avant la mise en place du SDK ne sont pas directement informées de l'intégration de celui-ci à l'application et de la finalité poursuivie par ce traitement.

Par conséquent, les personnes ne sont pas dûment informées de la collecte de leurs données de géolocalisation par la société TEEMO, *via* l'installation d'un SDK, à des fins de publicité ciblée.

En deuxième lieu, les utilisateurs des applications ne fournissent pas un consentement libre au traitement réalisé par la société.

Dans son avis n°15/2011 du 13 juillet 2011, le G29 considère que *Le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie […] Si les conséquences du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre .*

En l'espèce, la délégation a été informée que les applications des éditeurs partenaires utilisant le SDK n'existent pas sans celui-ci et que par conséquent, les personnes ne peuvent télécharger les applications mobiles sans télécharger le SDK. Ce traceur est donc indissociable des applications partenaires.

En conséquence, les utilisateurs des applications mobiles ne sont pas libres de consentir au traitement des données de géolocalisation réalisé par la société TEEMO, à partir des données transmises par les applications, l'utilisation de ces dernières impliquant automatiquement la transmission de données à ladite société.

En troisième lieu, il apparaît que les personnes ne fournissent pas un consentement spécifique au traitement mis en œuvre par la société TEEMO réalisé à des fins de profilage des utilisateurs et de ciblage publicitaire.

Dans un avis 15/2011 du 13 juillet 2011, le G29 a rappelé que : *Pour être valable, le consentement doit être spécifique. En d'autres termes, un consentement général, sans préciser la finalité exacte du traitement, n'est pas acceptable. Pour être spécifique, le consentement doit être intelligible. Il doit mentionner, de façon claire et précise, l'étendue et les conséquences du traitement des données […] Le consentement doit être donné sur les différents aspects, clairement définis, du traitement. […] En effet, il ne saurait être considéré comme couvrant toutes les finalités légitimes poursuivies par le responsable du traitement .*

La délégation a constaté à l'occasion du contrôle sur place que les personnes sont amenées à valider l'autorisation de collecter leurs données de géolocalisation uniquement pour l'utilisation de l'application mobile téléchargée. À titre d'exemple, s'agissant de l'application mobile […], au moment de l'installation de celle-ci, il est demandé à la personne de donner son accord de la manière suivante : *Autoriser […] à accéder à votre position ? Information pour toujours : pour profiter pleinement de l'application et vous proposer des contenus au plus proche de vos attentes.*

Les utilisateurs des applications mobiles partenaires ne consentent donc pas spécifiquement au traitement de leurs données de géolocalisation à des fins de profilage et de ciblage publicitaire.

Il résulte de tout ce qui précède que le consentement des personnes n'est pas valablement recueilli.

Les faits précités sont donc constitutifs d'un manquement aux dispositions de l'article 7 de la loi du 6 janvier 1978 modifiée.

Un manquement à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement
La délégation a été informée que le SDK installé dans les applications mobiles collecte les données de géolocalisation des utilisateurs environ toutes les cinq minutes. Ces données sont enregistrées dans les serveurs de la société et sont conservées durant treize mois puis purgées.

Une fois croisées avec les POIs recensés, les données de géolocalisation pertinentes sont ensuite intégrées dans la base de données Matcher2 et sont utilisées par la suite à des fins publicitaires. La délégation a constaté que les identifiants publicitaires des smartphones sur lesquels la publicité ciblée est effectuée sont conservés pendant treize mois au sein de la base de données Matcher2 .

Tout d'abord, la société a informé la délégation que lorsque le téléphone d'une personne est situé en dehors de la situation géographique des POIs recensés, aucune donnée n'est intégrée dans la base de données Matcher2 .

Dès lors, la conservation par la société de toutes les données de géolocalisation des utilisateurs au-delà du temps nécessaire à la réalisation de l'opération de correspondance entre les données collectées et les zones géographiques POIs - au sein desquelles la société effectue des campagnes marketing - est excessive au regard de la finalité de ciblage publicitaire du traitement.

En outre, dans sa déclaration normale n° 1873686, la société avait indiqué conserver les données de localisation des personnes *pendant la durée de la relation contractuelle .*

La durée déclarée à la CNIL n'est pas pertinente dès lors qu'aucun contrat n'est conclu entre la société et les utilisateurs des applications mobiles au sein desquelles les SDK sont intégrés.
Puis, lors du contrôle du 2 octobre 2017, la société a justifié la durée de conservation de treize mois des données de géolocalisation par la nature du service rendu par certains de ses partenaires et notamment ceux travaillant dans le secteur du voyage qui ont besoin de connaître les lieux visités par les personnes pendant cette durée.
La société ne peut justifier la conservation de l'intégralité des données de géolocalisation des personnes, durant treize mois, au motif que certains de ses partenaires pourraient avoir besoin de connaître les lieux visités par les mobinautes sur cette période. La conservation de telles informations constitue un risque d'atteinte à la vie privée des personnes concernées.

En effet, la Commission considère que l'utilisation des dispositifs de géolocalisation est particulièrement intrusive au regard des libertés individuelles, dans la mesure où ils permettent de suivre de manière permanente et en temps réel des personnes, aussi bien dans l'espace public que dans des lieux privés. Ainsi, la CNIL estime que les données de géolocalisation ne peuvent être conservées que pour une durée strictement proportionnée à la finalité du traitement qui a justifié cette géolocalisation.
Dès lors, quand bien même les conditions seraient réunies pour considérer que le traitement mis en œuvre dispose d'une base légale, la durée de conservation de treize mois de telles données est excessive au regard de sa finalité de profilage et de ciblage publicitaire.
Ces faits constituent un manquement aux dispositions de l'article 6-5° de la loi du 6 janvier 1978 modifiée qui prévoit que les données (…) *sont conservées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées et traitées* .

Il est en outre rappelé qu'en application des articles 226-20 et 226-24 du code pénal combinés, le fait pour une personne morale, de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni d'une peine d'amende pouvant atteindre 1.500.000 €.
Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données gérées par un sous-traitant

La délégation a été informée que les données des utilisateurs des applications mobiles collectées sont intégrées dans la base de données Matcher2 hébergée *via* les services de Google Cloud.

La délégation a cependant constaté que le contrat conclu entre la société TEEMO,

anciennement DATABERRIES, et la société Google ne prévoit pas de clauses relatives aux obligations du sous-traitant en matière de sécurité et de confidentialité des données à caractère personnel, précisant notamment que le sous-traitant ne peut agir que sur instruction du responsable de traitement.

Ces faits constituent un manquement aux dispositions de l'article 35 de la loi n° 78-17 du 6 janvier 1978 qui dispose notamment que *Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement* .

En conséquence, la société TEEMO, sise 39, Rue Godot de Mauroy à Paris (75009) est mise en demeure sous un délai de trois (3) mois à compter de la notification de la présente décision **et sous réserve des mesures qu'elle aurait déjà pu adopter, de :**

- **ne pas procéder sans base légale au traitement des données de géolocalisation des personnes à des fins de ciblage publicitaire, en particulier recueillir, de manière effective, le consentement préalable des utilisateurs des applications éditées par les partenaires de la société TEEMO au traitement de leurs données par cette dernière** (par exemple par la mise en place d'un pop-up contenant une information et une case à cocher dédiées) et à défaut, supprimer lesdites données collectées ;

- **sous réserve de base légale du traitement, définir et mettre en œuvre une politique de durée de conservation des données raisonnable**, en particulier :
- **supprimer les données de géolocalisation** des utilisateurs collectées en dehors des zones de POIs une fois la correspondance entre les données de géolocalisation et les zones de POIS effectuée ;
- **définir une durée de conservation des données de géolocalisation** proportionnée à la finalité du traitement et procéder à la purge ou, le cas échéant, à l'anonymisation des données anciennes ;

- **insérer une clause au sein du contrat conclu avec la société Google** précisant les obligations incombant à cette dernière en matière de sécurité et de confidentialité des données ;

- **justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.**

À l'issue de ce délai, si la société TEEMO s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la société TEEMO ne s'est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente

Isabelle FALQUE-PIERROTIN

[1]Il s’agit d’une annonce publicitaire qui s’affiche en plein écran et qui vient recouvrir la page visitée, dès la page d’accueil ou comme transition entre deux pages.
[2]Personne qui navigue sur Internet à partir d’un appareil mobile.
[3]Kit de développement logiciel.