SESSION Q&R AVEC LA CNIL
SUR LES NOUVELLES LIGNES DIRECTRICES
& RECOMMANDATIONS COOKIES

Document strictement réservé aux membres du GESTE

26/10/2020

Les éditeurs de contenus et services en ligne

GESTE

Etienne Drouard

Avocat Associé

Hogan Lovells

Clémence Scottez

Head of Economic sector department

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Armand Heslot

Head of technology experts department

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

SOMMAIRE

SUR LE CHAMP D'APPLICATION DES LIGNES DIRECTRICES

SUR LES MODALITÉS DE RECUEIL DU CONSENTEMENT

- Sur le caractère libre du consentement (Cookie Wall)
- Sur le caractère éclairé du consentement
- Sur la preuve du consentement
- Sur le refus et le retrait du consentement

SUR LA QUALIFICATION DES ACTEURS

SUR LES TRACEURS EXEMPTÉS DE CONSENTEMENT

AUTRES

- Sur la portée du consentement
- Sur la durée de vie de cookies

PRIVACY SHIELD

SUR LE CHAMP D'APPLICATION DES LIGNES DIRECTRICES

Dans quelles circonstances une adresse email (hachée) ou une adresse IP (tronquée) peuvent être considérées comme des traceurs en tant que tels, entrant dans le champ d'application des nouvelles lignes directrices de la CNIL du 17 septembre 2020 ?

Une adresse email hachée et/ou une adresse IP tronquée peuvent être utilisées comme des traceurs. Tout dépend du contexte. Si il y a lecture ou écriture d'une adresse email hachée dans le terminal de l'utilisateur, via un cookie ou une autre technique qui constitue une opération de lecture ou d'écriture, il faut faire application de l'article 82 (qui s'applique même s'il n'y a pas de données personnelles), des Lignes directrices et de la Recommandation. Cela ne signifie pas que d'une manière générale, l'usage d'une adresse email ou d'une adresse IP nécessite un consentement. La CNIL s'attache à la nature de l'opération.

La lecture seule d'un traceur (sans dépôt), sur un serveur d'un acteur économique tiers (non pas dans l'équipement terminal de l'utilisateur), peut-elle être considérée comme une opération rentrant dans le champ d'application des nouvelles lignes directrices de la CNIL ?

Non. La directive ePrivacy, l'article 82, les lignes directrices et la recommandation ne s'appliquent qu'aux opérations de lecture et d'écriture dans le terminal de l'utilisateur. Si des donnés sont lues ou échangées entre des serveurs "en back office" sans passage par le terminal de l'utilisateur, l'article 82 ne s'applique pas.

Qu'en est-il des actions "autres" ou postérieures au dépôt et à la lecture ? Par exemple lorsqu'un identifiant peut être inséré sous forme de macro dans le libellé d'une url associée à un pixel transparent ? Comment pourrait-on se prévaloir d'un régime d'information et de recueil du consentement pour le dépôt de cet identifiant dans le terminal d'un utilisateur afin que le transport de cet identifiant dans l'url d'un pixel puisse être réputé avoir reçu un consentement ?

Dans ce cas de figure il y a bien à la source une lecture d'information dans le terminal. Il faut pouvoir extraire l'identifiant cookie pour le mettre dans un URL et donc obtenir un consentement. La consultation de l'URL n'est pas réellement une opération de lecture ou d'écriture mais, à la source, il y a bien une opération soumise au consentement. Sur ce point, la CNIL renvoie à sa FAQ et recommande aux éditeurs d'adresser leurs questions afin que l'Autorité puisse faire évoluer sa FAQ sur son site.

Point 14 des lignes directrices

Certains cookies, permettant de répondre à une obligation légale semblent être exclus du régime d'exemption (mesure d'audience publicitaire, lutte contre la fraude). Pourtant, les soumettre à un régime d'opposition ou de consentement préalable reviendrait à empêcher l'éditeur de répondre à ses obligations légales ou contractuelles.

Faut-il soumettre ces cookies au consentement ePrivacy quitte à se mettre en défaut par rapport à nos obligations légales ou contractuelles ? Autrement dit, La CNIL confirme-t-elle permettre à l'utilisateur de ne pas consentir à une collecte pour des traitements rendus légalement ou contractuellement obligatoires ?

Peut-on considérer les cookies nécessaires pour les traitements ultérieurs ayant pour base légale le respect d'une obligation légale comme étant exemptés du consentement ?

- La liste des cookies exemptés n'est pas exhaustive.
- La CNIL observe qu'aucune loi ne prévoit l'obligation de déposer des cookies. Aucun texte n'implique l'usage de cette technique pour répondre à une obligation légale. Le Conseil d'Etat a imposé à la CNIL d'avoir une vision très restrictive de la liste des cookies exemptés afin de respecter au maximum les conditions de l'article 82, c'est à dire le cookie nécessaire à la fourniture du service expressément demandé par l'utilisateur.
- Le régime du RGPD ne permet pas de s'exonérer de l'obligation d'appliquer la directive ePrivacy. Il n'y a aucune exemption liée à une exécution d'une obligation légale ou contractuelle.

Point 15 des lignes directrices

Pouvez-vous expliquer le point 15 des lignes directrices sur les conséquences pratiques de la distinction que vous faites entre le traceur et les traitements portant sur les données collectées par un traceur ?

Exemple du traitement d'Onboarding : En matière publicitaire, le traitement utilise des données qui proviennent d'un cookie et des données qui proviennent d'autres traitements de données. Ce traitement est alimenté par l'opération de lecture et d'écriture de données qui sont collectées via l'opération de lecture et d'écriture, et doit être traité comme un traitement en tant que tel, soumis au RGPD.

La CNIL recommande un raisonnement en deux temps :

- Temps 1 : Quelle est l'opération par laquelle les données sont obtenues, est-elle soumise au consentement ePrivacy ?
- Temps 2 : Voir le traitement dans son ensemble "Quelles sont les données qui intègrent ce traitement ?" et de quelle manière le RGPD permet de les traiter ?

Théoriquement si la première opération consistant à traiter un identifiant relève bien du régime des cookies et traceurs - donc du consentement des personnes - les traitements ultérieurs dans lesquels cet identifiant peut être intégré peut avoir une autre base légale **MAIS** ce qui ressort des derniers avis est une **préférence forte pour le recours au consentement** en tant que base légale du RGPD, en raison du caractère intrusif de la technique de collecte via les traceurs.

SUR LES MODALITÉS DE RECEUIL DU CONSENTEMENT

Sur le caractère libre du consentement (Cookie Wall)

Quelles pourraient être les bonnes pratiques en matière d'alternative d'accès à un service ? Est-ce que la voie d'une double entrée au contenu par exemple cookie wall / paywall ou log in wall pourrait être envisagée ? / La doctrine de la CNIL accepte-t-elle qu'en cas de refus de consentement, le service proposé ne soit pas exactement celui offert aux internautes ayant accepté les cookies ? / Quels sont les critères qui permettent à la CNIL d'apprécier la licéité des conditions alternatives d'accès à un service en cas de refus ou de retrait du consentement ? En raison de l'incertitude posée par l'analyse au cas par cas, quels conseils pouvez-vous donner aux éditeurs ? / L'usage de la pratique du cookies wall est-il justifié pour tous les cookies toutes finalités confondues (ex. à des fins de mesure d'audience, personnalisation de contenus) ou uniquement pour des cookies publicitaires ? / Concernant le cookie wall, est-ce que l'alternative « payante » proposée en cas de refus ou retrait du consentement, renvoyant l'utilisateur vers un tiers n'utilisant pas de cookies, distributeur autorisé des contenus de l'éditeur, est une possibilité envisageable pour la CNIL ?

Le Conseil d'Etat ouvre la possibilité du Cookie Wall. **A ce stade la Commission n'envisage pas de proposer de bonnes pratiques ni de travailler sur l'étude de critères alternatifs. La CNIL recommande de ne pas mettre en place de CW, même s'il ne lui appartient pas d'interdire cette pratique**. La CNIL indique que c'est aux acteurs concernés de s'interroger sur les critères à respecter.

La CNIL indique que, si elle devait travailler sur de tels critères, cela nécessiterait une harmonisation européenne. Il y aurait alors plusieurs difficultés, notamment en raison de la transposition et de l'interprétation différente d'ePrivacy au sein de chaque Etat Membre. Par ailleurs, il n'appartient pas à l'EDPB de définir les critères de validité d'un CW (l'EDPB ayant déjà considéré que le CW était illicite).

La CNIL relève que les questions adressées sont légitimes et pertinentes et les remontera aux Commissaires Rapporteurs. L'Autorité ne sait pas encore si la clarification des critères pourra se faire à l'occasion du démarrage des contrôles ou des actions contentieuses au cas par cas, ou encore si elle sera en mesure de répondre précisément à chacune des questions en amont...

Autre piste pour s'assurer de la validité du CW par la CNIL : Via une analyse d'impacts soumise à l'Autorité sur la base de l'article 36 en présence d'un risque résiduel élevé lié au CW à laquelle elle serait alors contrainte de répondre.

Sur le caractère éclairé du consentement

La recommandation consistant à afficher l'ensemble des responsables des traitement des opérations de lecture et d'écriture ne tient pas compte du fonctionnement du programmatique, quelle est la marge de manœuvre des éditeurs sur ce point ? En effet, dans la publicité programmatique, l'éditeur ne connaît pas à l'avance l'ensemble des acteurs intervenants pour un utilisateur donné, la liste des destinataires devra donc être potentielle, c'est-à-dire probablement plus large que la réalité. Cela aura plus pour conséquence d'inquiéter que de fournir une information pour un consentement éclairé.

A quelle fréquence cette liste doit-elle être mise à jour ? Quelles sont les conséquences d'un délai de mise à jour considéré comme trop long ? Faut-il stocker chaque version de chaque liste et sa période de publication ? Si oui, pourquoi ?

Si les informations spécifiques concernant les responsables de traitement peuvent être fournies à un second niveau d'information (via un lien hypertexte ou un bouton), quelles sont les informations devant nécessairement être fournies au premier niveau d'information ? (point 19 de la recommandation)

Sur la preuve du consentement

Quelle granularité dans la preuve du consentement ? Etant donné que la rédaction sur la preuve « individuelle » du recueil d'un consentement valide a disparu dans la version adoptée de la recommandation CNIL du 17 septembre 2020, confirmez-vous qu'il n'est plus nécessaire pour les éditeurs de mettre au point un dispositif enregistrant, individu par individu : un horodatage du consentement, le contexte dans lequel le consentement a été recueilli (identification du site web ou de l'application mobile), le type de mécanisme de recueil du consentement utilisé, et les finalités auxquelles l'utilisateur a consenti.

La preuve « individuelle » (et le respect de l'obligation de conserver/enregistrer les choix de l'utilisateur) correspond-elle désormais à uniquement nommer le traceur permettant de stocker le choix des utilisateurs « eu-consent », en attachant à chaque finalité une valeur booléenne « vrai » ou « faux » mémorisant les choix effectués ?

Sur le caractère éclairé du consentement / Sur la preuve du consentement

Le Conseil d'Etat a indiqué que le Responsable de Traitement doit être en mesure de fournir à tout moment la preuve du recueil valable du consentement de l'utilisateur. Une absence de mise à jour de la liste sera totalement préjudiciable notamment pour le RT tiers qui ne se serait pas déclaré comme étant responsable de traitement pour figurer dans la liste. La CNIL est consciente des difficultés de l'exercice toutefois, elle rappelle que juridiquement l'obligation est de fournir une liste mise à jour.

Pour l'Autorité la question de la fréquence de cette mise à jour n'a pas lieu d'être : au moment où l'utilisateur consent, soit le tiers qui réalise un opération de lecture et d'écriture était présent dans la liste auquel cas le consentement est valable, soit il ne l'était pas et alors il ne peut pas se prévaloir du consentement.

Pour le démontrer, tout dépend du type de solution technique implémentée pour obtenir le consentement.

- Dans le mécanisme du TCF par exemple, l'utilisateur donne son consentement qui est ensuite attribué à chacun des acteurs présents au moment où il a donné son consentement. Les nouveaux acteurs qui se retrouveront dans la liste n'auront pas le consentement tant que l'utilisateur n'aura pas consenti à nouveau.
- Dans une solution de tag manager il faut que l'éditeur soit capable de démontrer le consentement et donc de prouver à tout moment que lorsqu'une opération de lecture et écriture est réalisée par un tiers, l'internaute a bien donné son consentement à ce tiers (voir notamment l'exemple du site de la CNIL).

La CNIL renvoie au point 29 des Lignes directrices : Passage sur la preuve du consentement qui impose une preuve unitaire. La recommandation précise comment procéder.

Comment la CNIL procèdera t-elle? L'autorité se rendra sur un site web et prendra une copie de la liste des entités susceptibles d'avoir recours à un opération de lecture et d'écriture soumise au consentement puis observera si d'autres entités viennent procéder à des opérations de lecture et d'écriture.

DONC selon le mécanisme de consentement choisi, l'éditeur devrait seul ou avec un mécanisme externe conserver la preuve - pour chaque identifiant cookie- d'une date et d'une heure à laquelle une information a été fournie à l'utilisateur s'agissant des finalités acceptées, de la liste des acteurs déposant des cookies et des traceurs portée à la connaissance de l'utilisateur afin de permettre aux tiers ou lui-même de se prévaloir de l'information fournie aux personnes. Il faut donc être en mesure d'historiser chacune des versions de la liste.

Sur le refus et le retrait du consentement

Sachant qu'il doit être aussi facile de consentir que de refuser le dépôt de cookie, la nouvelle typologie de CMP proposée par la CNIL et les précisions quant aux modalités d'expression du refus, ne sont-elles pas de nature à créer une asymétrie dans le régime d'acceptation et de refus, en faveur du refus ? La CNIL peut-elle préciser le fondement légal de cette obligation ?

Les LD indiquent que le refus de l'utilisateur peut se déduire de son silence. A l'inverse, peut- il être forcé à faire un choix entre tout accepter / tout refuser / paramétrer ?

S'agissant de l'absence de consentement, nous avons compris que la CNIL souhaite qu'il soit appréhendé comme un refus. Néanmoins, la fonctionnalité de fermer la fenêtre est perçue comme celle de ne pas s'exprimer par l'internaute et d'accéder au site. Peut-on imaginer représenter à l'internaute une modale de consentement à une fréquence supérieure à celle de l'expiration de son consentement et calculée en fonction de son passage (toutes les x fois) ou sur une durée calendaire liée à l'activité du site ou en cas de changement substantiel lié aux finalités et/ou destinataires ?

La CNIL peut-elle fournir d'autres exemples de modèle de consentement qu'elle considèrerait comme valide ?

L'absence de consentement devant être considérée comme un refus, quel est l'impact du régime du non-consentement sur les autres bases légales définies par le RGPD, comme l'intérêt légitime ?

La CNIL envisage-t-elle d'imposer une symétrie des durées de conservation du silence/refus et du consentement ? Si oui, sur quel fondement légal ?

Quels sont les critères pouvant influer sur la durée d'enregistrement du refus ou du consentement ? Il est indiqué que la nature ou l'audience du site peut influer, qu'entendez- vous par là ? Que signifie le terme «spécificité de son audience» pour un site web ? (point 37 des recommandations)

Explications de la CNIL sur le fait que le refus peut être exprimé via un silence : Le consentement doit se faire via un acte positif. Le consentement permet d'ouvrir une porte qui est fermée par défaut. Sans action, la porte reste close.

L'éditeur peut imposer à une personne de répondre, cela n'est pas interdit par le RGPD.

Concernant la symétrie des durées de conservation : La CNIL indique qu'il n'y a pas forcément d'exigence de symétrie entre la durée de conservation du consentement et du refus. La borne inférieure de la durée de conservation du refus ou du non consentement ne dépend pas du contexte mais de savoir si cela est susceptible de constituer un harcèlement vis-à-vis de la personne (exemple: sollicitation sur toutes les pages).
Il est donc possible d'envisager une conservation du refus pour des durées variables en fonction du contexte dans lequel il est émis. **L'éditeur devrait s'assurer que la durée de conservation du refus n'est pas susceptible d'altérer la liberté du consentement**. La CNIL précise qu'il faut distinguer les sites sur lesquels un utilisateur revient régulièrement et ceux visités de manière occasionnelle.

Chaque éditeur doit construire son propre argumentaire justifiant de la durée de conservation du consentement ou du non-consentement / refus.

SUR LA QUALIFICATION DES ACTEURS

Dans le projet initial de recommandation : «14. [....] l'éditeur [...] y compris par des tiers, [...] devrait s'assurer de la présence d'un mécanisme permettant de recueillir le consentement [...] s'agissant des opérations de lecture et/ou d'écriture [...]»Cette définition limitative en droit souple de la responsabilité de l'éditeur a disparu dans les nouvelles recommandations. Cela remet-il en cause ce rôle de l'éditeur pour le mécanisme de collecte ou l'étendrait-il à des contrôles sur des traitements dont il n'a pas connaissance ? Dès lors que l'éditeur s'est assuré de respecter ses obligations concernant les cookies tiers déposés sur son site internet (s'assurer que ses partenaires n'émettent pas des traceurs qui ne respectent pas la réglementation applicable et effectuer toute démarche utile auprès d'eux pour mettre fin à ces manquements), peut-il néanmoins être tenu en partie responsable en cas de plainte d'un utilisateur portant sur les cookies tiers ? En effet, seul l'éditeur a un contact direct avec l'utilisateur.

La suppression de cette phrase n'était pas voulue, il s'agissait de remanier la partie relative aux responsabilités pour restituer l'éclairage obtenu du Conseil d'Etat et de la CJUE sur les rôles des chacun. La logique reste celle de la co-responsabilité notamment concernant le recueil du consentement. Si un tiers détourne la finalité déclarée à l'éditeur, la responsabilité de l'éditeur pourra très difficilement être recherchée. En effet, la co-responsabilité se situe sur ce qui est à la portée de l'éditeur. L'éditeur devrait clarifier avec un maximum d'acteurs, notamment le premier cercle d'acteurs avec lequel il est en contact, la répartition des responsabilités. Le contrat permet de faire une distribution des obligations de chacun, à condition qu'il ne soit pas totalement disproportionné en faveur ou à l'encontre d'une partie et qu'il correspond à la réalité.

Les éditeurs sont amenés à afficher sur leurs sites des publicités pour des annonceurs avec lesquels ils ont des partenariats, et qui dépendent par exemple non pas du tracking de l'internaute mais du contexte rédactionnel. La publicité n'est pas ciblée. Cependant, ces publicités intègrent des trackers qui permettent à l'annonceur d'analyser l'efficacité de ses campagnes. L'éditeur est-il responsable de collecter le consentement pour ces trackers?

Oui, car l'utilisation des traceurs est conjointe entre l'éditeur et l'annonceur. L'utilisation de ces traceurs doit être encadrée contractuellement.

La CJUE (Fashion ID ? Planet 49) précise qu'il incombe au régulateur de déterminer au cas par cas les responsabilités respectives des acteurs susceptibles d'être qualifiés de responsables conjoints. La recommandation présume la responsabilité conjointe sans fournir de piste sur les responsabilités distinctes ? Quels critères peuvent-ils être retenus par la CNIL ?

Les lignes directrices sur la qualification des parties soumises à consultation par l'EDPB vont dans le sens d'une approche pragmatique. La CNIL insiste : une forme de complicité par rapport à des faits que l'éditeur ne connaissait pas est difficile à retenir.

SUR LES TRACEURS EXEMPTÉS DE CONSENTEMENT

La CNIL devrait clarifier le sens du terme «utiliser» mentionné au §48 des lignes directrices : est-ce que ce terme fait référence à l'écriture, à la lecture de cookie ou à ces deux opérations ?

Il s'agit des deux opérations. La CNIL utilise ce terme pour englober le cas des cookies utilisés pour plusieurs finalités (dont certaines peuvent être exemptées et d'autres non). Cela n'exonère donc pas d'obtenir le consentement pour la finalité non exemptée.

Doit-on comprendre des nouvelles lignes directrices que le cookie de mesure d'audience, lorsqu'il est exempté du consentement, n'est pas soumis à un régime d'opposition ad hoc ?

La CNIL a supprimé volontairement le régime d'opposition ad hoc de ces lignes directrices. Il n'y a plus d'obligation de recueillir le consentement préalable pour ces cookies qui entrent dans le cadre de l'exemption. La CNIL considère que les traitements de mesure d'audience qui utilisent des cookies exemptés restent soumis au RGPD et donc à un droit d'opposition.

Concernant les critères d'exemption, il est indiqué que les traceurs "doivent avoir une finalité strictement limitée à la seule mesure d'audience sur le site ou l'application", quid des environnements logués et de l'environnement applicatif où tout repose sur un seul identifiant ?

La CNIL renvoie à l'article 6 de la Recommandation. Il s'agit d'une simple recommandation, cela ne signifie pas qu'il y ait automatiquement une sanction. Attention toutefois, la CNIL précise que si un cookie est déposé sans consentement alors qu'il n'est pas strictement nécessaire, le manquement sera, bien sûr, susceptible d'être sanctionné par la CNIL. Par ailleurs, l'Autorité observe que, sur les identifiants mobiles, il n'est pas impossible de scinder les finalités. Par exemple, sur iOS, il existe plusieurs jeux d'identifiants (ID publicitaire qui n'a vocation à servir qu'à la publicité / ID par application qui a vocation à servir d'ID au sein d'une seule et même application / ID transverse à un même éditeur de logiciel de différentes applications)

Aucune exemption n'est retenue pour les cookies techniques utilisés pour la publicité. Ces cookies n'ont pas d'enjeu vie privée, ils ne s'intéressent pas au profil de l'internaute qui va visualiser les publicités. Sans ces cookies il n'est pas possible d'avoir une activité publicitaire non ciblée. Doit-on comprendre que l'exemption ne s'applique pas aux obligations de comptage des espaces publicitaires strictement nécessaires pour pouvoir faire de la publicité sur nos sites ?

La CNIL considère qu'il y a **une seule et même finalité** : "Afficher de la publicité" et ne distingue pas de finalités liées à la performance, au capping, à la mesure d'audience publicitaire, lutte contre la fraude … Pour la CNIL il s'agit bien d'opérations de traitement qui entrent dans cette seule et même finalité. Il peut y avoir un seul cookie utilisé pour l'ensemble de ces opérations mais ce cookie nécessite un consentement. La CNIL confirme qu'**il n'y a pas d'exemption pour des opérations de traitement qui relève de la publicité ciblée**.
Dans le cas où tous les traitements reposent sur du contextuel, l'Autorité recommande de l'indiquer clairement aux utilisateurs dans la mesure où l'intrusion est limitée.

Les traceurs permettant de réaliser les AB Test sur les sites d'un éditeur n'apparaissent plus dans la doctrine, or ils étaient cités précédemment dans les lignes directrices de juillet 2019. Doit-on en conclure que l'opinion de l'Autorité sur ces traceurs a changé ? Quelle serait la conséquence pour le dépôt desdits traceurs ?

Oui, les AB tests ne sont plus exemptés de consentement.

Point 51 : est-ce que l'exigence que la mesure d'audience soit "pour le compte exclusif de l'éditeur" fait obstacle à ce que l'éditeur partage des rapports statistiques/agrégés issus du traitement de mesure mise en œuvre avec des tiers sans accès des tiers à des données à caractère personnel ? avec des sous-traitants ?

Non, à partir du moment où il s'agit de pures statistiques, elles peuvent être partagées à des tiers ou des sous-traitants.

AUTRES

Sur la portée du consentement

Dans ses nouvelles recommandations, la CNIL indique que lorsque les traceurs sont déposés par d'autres entités que l'éditeur, et permettent un suivi de la navigation de l'utilisateur au-delà du site où les traceurs ont initialement été déposés, elle recommande fortement que le consentement soit recueilli sur chacun des sites concerné par la navigation. Le paragraphe suivant de la précédente version des recommandations a disparu, à savoir : « pour qu'un consentement recueilli sur un site ou une application mobile soit également valide sur d'autres sites ou applications mobiles, la liste de la totalité des sites web ou applications mobiles concernés peut être rendue accessible via un lien hypertexte ou un bouton situé sur le premier niveau du mécanisme de recueil du consentement ».

- Par conséquent, quid du recueil du consentement par un éditeur sur l'un de ses sites et de sa validité sur les autres sites ?

- Au surplus, quid de la validité du consentement pour différents sites d'un même Groupe ?

La CNIL renvoie au point 17 des recommandations mais indique que tout dépend du contexte.

La personne concernée doit être informée de l'identité des responsables de traitement et doit avoir conscience de l'ensemble des sites qui pourraient bénéficier de son consentement via, par exemple, un lien hypertexte renvoyant à la liste des sites concernés. De cette manière, le consentement est valable.

Attention, **le retrait du consentement doit alors être répercuté sur l'ensemble des sites.**

La CNIL indique que cela est plus délicat dans le cadre d'une régie qui a une multitude de clients, eux-même des groupes. Dans ce cas de figure, l'information sera difficile à indiquer de manière claire et probante.

Idem concernant le consentement multisupport / cross device : il faut être clair sur les supports concernés et s'assurer que le retrait du consentement soit effectif sur l'ensemble des supports.

Sur la durée de vie de cookies

La durée de vie de 13 mois pour les cookies et traceurs déposés sur le terminal de l'utilisateur permettait une appréciation générale et une homogénéisation des durées appliquées par les acteurs pour les traceurs non intrusifs, des durées plus courtes devant selon la doctrine de la CNIL être adoptées pour les traceurs créant un risque avéré pour les personnes concernées (géolocalisation précise par exemple). La durée de vie des cookies n'apparaît plus que pour le cookie de mesure d'audience exempté de consentement, seule une bonne pratique de conservation du choix de 6 mois est précisée (Recommandation 39).

- Cela veut-il dire que la durée de vie des cookies de 13 mois disparaît suite à l'abrogation de la délibération du 5 dec. 2013 ?

- La commission confirme-t-elle que la durée de vie des cookies doit maintenant être considérée eu égard aux finalités poursuivies et donc qu'il est possible pour les traitements dont la durée serait supérieure à 13 mois et nécessitant l'implantation de cookies et traceurs ?

La durée de vie des cookies est plutôt liée à la profondeur historique des données que l'éditeur est susceptible de collecter via un même identifiant mais pas forcément liée à la durée de conservation qui elle-même s'appliquerait aux données collectées par l'intermédiaire des cookies.

La CNIL revient donc à un point fondamental : la durée de vie des cookies doit être adaptée à la finalité de l'opération de lecture et d'écriture. Le délai de 13 mois n'est donc plus d'actualité mais chaque responsable de traitement doit être en mesure de justifier de la durée de vie du cookie et de la mettre en perspective avec la profondeur historique des données dont ils ont besoin par rapport à la finalité fixée.

PRIVACY SHIELD

Est-ce que la signature des CCT, en l'état, avec nos partenaires sous Privacy Shield est suffisante dans un premier temps ?

Les CCT doivent être prises en compte mais ne permettent pas de pallier au fait que ce qui est contractuellement opposable à l'autre partie ne l'est pas au gouvernement américain. In fine, les CCT ne se suffisent pas à elles-mêmes d'où la nécessité d'identifier tous les transferts potentiels de données vers des pays ne fournissant pas un niveau de protection suffisant et voir si :

La CNIL recommande donc de :

- Mapper les transferts et identifier s'ils sont véritablement nécessaires ;
- Identifier les outils d'encadrement ;
- Identifier si l'article 49 peut être mobilisé **Attention** cet article permet de valider de **manière ponctuelle** des transferts sur la base d'exemptions tels que le consentement, l'intérêt public, le contrat … mais la CNIL rappelle que cela ne fonctionne que **si le transfert n'est pas systémique**. Or, les transferts relatifs aux traceurs sont souvent systémiques ;
- Identifier les mesures juridiques et techniques à mettre en place.

Attention, l'Autorité rappelle que la CJUE n'a pas donné de délai de grâce aux responsables de traitement.

En quoi des flux d'identifiants stockées dans des serveurs tombent sous le coup des lois pour lesquelles la CJUE a estimé qu'une protection devait être assortie de garanties supplémentaires ? Quid du régime applicable aux cookies ? Tombent-ils sous les lois de surveillance américaines ?

Oui, **la publicité digitale est concernée par l'arrêt de la CJUE.**

La CNIL indique qu'à partir du moment où l'on transfert des données liées à des identifiants cookies hors de l'UE, Schrems II s'applique.

Les lois de surveillance américaines ne s'appliquent pas à des activités mais à **des typologies d'acteurs**.

En l'état actuel des réflexions, différents types d'acteurs sont soumis à différentes lois comme :

- le cloud act qui concerne tous les acteurs et les données stockées en dehors des USA permettant d'identifier un individu (y compris les identifiants cookies) ;
- le visa executive order qui cible des acteurs particuliers (fournisseurs de service de télécommunications).

Les acteurs européens doivent s'interroger : La donnée est-elle transmise par un fournisseur de service de télécommunication ? Si oui, **le simple fait que la donnée transmise à un acteur le soit par l'intermédiaire d'un service de télécommunication, la rend accessible aux autorités judiciaires et de renseignement américaines** et rend donc le **transfert illicite.**

Les éditeurs de contenus et services en ligne

GESTE

76 rue Richelieu, 75002 Paris
www.geste.fr

01 47 03 04 60
sara@geste.fr