Publié le 11 mars 2021 par **Laure Marolleau**, Avocat au Barreau de Paris
l.marolleau@soulier-avocats.com
Tél. : + 33 (0)1 40 54 29 29

Lire cet article en ligne

Cookies et traceurs : vos sites internet et applications mobiles sont-ils en conformité ?

Lorsqu'ils visitent un site web ou utilisent des applications mobiles, les utilisateurs doivent être informés et donner leur consentement préalablement au dépôt ou à la lecture de cookies ou autres traceurs, à moins que ces traceurs ne bénéficient d'une des exemptions prévues par la loi.

A la suite de la publication de ses lignes directrices et de sa recommandation le 1er octobre 2020, la CNIL a laissé jusqu'au 31 mars 2021 pour mettre les sites web et applications mobiles en conformité avec les nouvelles règles.

Qu'est-ce qu'un cookie ou un traceur ?

Les termes de « cookie » ou « traceur » recouvrent par exemple :

- les cookies HTTP,
- les cookies « flash »,
- le résultat du calcul d'une empreinte unique du terminal dans le cas du « fingerprinting » (calcul d'un identifiant unique du terminal basé sur des éléments de sa configuration à des fins de traçage),
- les pixels invisibles ou « web bugs »,
- tout autre identifiant généré par un logiciel ou un système d'exploitation (numéro de série, adresse MAC, identifiant unique de terminal (IDFV), ou tout ensemble de données qui servent à calculer une empreinte unique du terminal (par exemple via une méthode de « fingerprinting »).

Ils peuvent être déposés et/ou lus, par exemple lors de la consultation d'un site web, d'une application mobile,

ou encore de l'installation ou de l'utilisation d'un logiciel et ce, quel que soit le type de terminal utilisé : ordinateur, smartphone, tablette numérique ou console de jeux vidéo connectée à internet.

Que dit la loi ?

L'article 5(3) de la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques, dite e-privacy, pose le principe :

- d'un consentement préalable de l'utilisateur avant le stockage d'informations sur son terminal ou l'accès à des informations déjà stockées sur celui-ci ;
- sauf si ces actions sont strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique.

L'article 82 de la loi Informatique et Libertés, qui transpose ces dispositions en droit français, prévoit :

« 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. »

La CNIL rappelle que le consentement prévu par ces dispositions renvoie à la définition et aux conditions prévues aux articles 4(11) et 7 du RGPD. Il doit donc être libre, spécifique, éclairé, univoque et l'utilisateur doit être en mesure de le retirer, à tout moment, avec la même simplicité qu'il l'a accordé.

Afin de rappeler et d'expliciter le droit applicable au dépôt et à la lecture de traceurs dans le terminal de l'utilisateur, la CNIL a adopté le 17 septembre 2020 des lignes directrices[1] et une recommandation[2]. Elle a accordé 6 mois aux entreprises pour se mettre en conformité, soit au plus tard le 31 mars 2021.

Quels cookies nécessitent un consentement préalable ?

Tous les cookies n'ayant pas pour finalité exclusive de permettre ou faciliter une communication par voie électronique ou n'étant pas strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur nécessitent le consentement préalable de l'internaute.

Parmi les cookies nécessitant une information préalable et le recueil préalable du consentement de l'utilisateur, on peut notamment citer :

- les cookies liés aux opérations relatives à la publicité personnalisée ;
- les cookies des réseaux sociaux, notamment générés par leurs boutons de partage.

Parmi les traceurs non soumis au consentement, on trouve notamment :

- les traceurs conservant le choix exprimé par les utilisateurs sur le dépôt de traceurs ;
- les traceurs destinés à l'authentification auprès d'un service, y compris ceux visant à assurer la sécurité du mécanisme d'authentification, par exemple en limitant les tentatives d'accès robotisées ou inattendues ;
- les traceurs destinés à garder en mémoire le contenu d'un panier d'achat sur un site marchand ou à facturer, à l'utilisateur, le(s) produit(s) et/ou service(s) acheté(s) ;
- les traceurs de personnalisation de l'interface utilisateur (par exemple, pour le choix de la langue ou de la présentation d'un service), lorsqu'une telle personnalisation constitue un élément intrinsèque et attendu du service ;
- les traceurs permettant l'équilibrage de la charge des équipements concourant à un service de communication ;
- les traceurs permettant aux sites payants de limiter l'accès gratuit à un échantillon de contenu demandé par les utilisateurs (quantité prédéfinie et/ou sur une période limitée) ;
- certains traceurs de mesure d'audience dès lors qu'ils respectent certaines conditions.

Comment recueillir un consentement valable ?

Le consentement doit se manifester par une action positive de la personne préalablement informée, notamment, des conséquences de son choix et disposant des moyens d'accepter, de refuser et de retirer son consentement.

Des systèmes adaptés doivent donc être mis en place pour recueillir le consentement selon des modalités pratiques qui permettent aux internautes de bénéficier de solutions simples d'usage.

La CNIL fournit des exemples de mise en œuvre dans sa recommandation.

Ce qu'il faut retenir :

- **le consentement doit être préalable au dépôt et/ou à la lecture de cookies**. Autrement dit, tant

que la personne n'a pas donné son consentement, les cookies ne peuvent pas être déposés ou lus sur son terminal ;

- **le consentement est une manifestation de volonté, libre, spécifique, univoque et éclairée**. La validité du consentement est donc notamment liée à la qualité de l'information reçue. Concrètement, elle doit être visible, mise en évidence, rédigée en des termes simples et compréhensibles par tout utilisateur. Il est possible d'avoir deux niveaux d'information : par exemple, un premier niveau peut brièvement décrire chaque finalité de traitement, puis un second niveau fournir plus de détails sur ces finalités et sur la liste des responsables du ou des traitements ;
- **le consentement n'est valide que si la personne exerce un choix réel**. L'utilisateur doit pouvoir accepter ou refuser le dépôt et/ou la lecture des cookies avec le même degré de simplicité.
- **le consentement doit pouvoir être retiré simplement et à tout moment par l'utilisateur.** Concrètement, des solutions permettant aux utilisateurs de retirer leur consentement doivent être mises à la disposition de l'utilisateur et accessibles à tout moment.

Comment prouver le consentement ?

Attention, il faut être en mesure d'apporter la preuve du consentement !

La CNIL donne quelques exemples pour le faire :

- mise sous séquestre auprès d'un tiers du code informatique utilisé par l'organisme recueillant le consentement, pour les différentes versions de son site ou de son application mobile, voire simplement par la publication horodatée sur une plate-forme publique d'un condensat (ou « hash ») de ce code pour pouvoir prouver son authenticité a posteriori ;
- une capture d'écran du rendu visuel affiché sur un terminal mobile ou fixe peut être conservée, de façon horodatée, pour chaque version du site ou de l'application ;
- des audits réguliers des mécanismes de recueil du consentement mis en œuvre par les sites ou applications depuis lesquels il est recueilli peuvent être mis en œuvre par des tiers mandatés à cette fin ;
- conservation horodatée, par les tiers éditant ces solutions, des informations relatives aux outils mis en œuvre et à leurs configurations successives (tels que les solutions de recueil du consentement, également connues sous l'appellation CMP « Consent Management Platform »).

Quel risque ?

L'article 20 de la loi Informatique et Libertés liste les différentes mesures et sanctions que la CNIL peut prononcer en cas de manquement.

S'il s'agit d'une amende, il est prévu qu'elle ne peut excéder 10 millions d'euros ou 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 RGPD (qui comprennent notamment les règles en matière de consentement et les droits des personnes), ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires.

La CNIL prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

---

[1] Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019. Cf. notre article intitulé Nouvelles lignes directrices de la CNIL sur les cookies publié sur notre Blog au mois de septembre 2019. Elles ont été ajustées pour tirer les conséquences de la décision rendue le 19 juin 2020 par le Conseil d'Etat.

[2] Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ». Cf. notre article intitulé Recommandation de la CNIL sur les cookies publié sur notre Blog au mois de janvier 2020.