Consentement des internautes : cookies et autres traceurs sont dans le viseur de la Cnil, Europe oblige

Sont parues le 19 juillet au *Journal Officiel* les lignes directrices de la Cnil concernant les « *opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs)* », en attendant ses recommandations pour début 2020, et le futur règlement « ePrivacy » européen.

Par Olivia Roche, avocate, et Prudence Cadio, avocate associée, cabinet LPA-CGR avocats

L'utilisation des cookies et autres traceurs est actuellement encadrée par la directive européenne dite « ePrivacy » (1), plusieurs fois modifiée, notamment par la directive de 2009 renforçant l'obligation d'information des internautes et leur consentement (2). Si cette dernière a vocation à être abrogée et remplacée par le règlement européen « ePrivacy » (3), celui-ci est toujours en discussion devant les instances européennes.

Toutefois, l'entrée en vigueur en mai 2018 du RGPD – règlement général sur la protection des données du 27 avril 2016 – a permis un premier pas vers la modernisation des règles entourant l'utilisation de traceurs et cookies.

Le consentement doit être *« éclairé »*

Dans cette lignée, la Commission nationale de l'informatique et des libertés (Cnil) a d'ores et déjà anticipé les changements à venir, forçant ainsi les acteurs du secteur de la publicité en ligne à prévoir une évolution très prochaine de leurs pratiques. Pour se mettre en conformité avec le RGPD, l'ordonnance du 12 décembre 2018 a abrogé l'article 32-II de la loi relative à l'informatique, aux fichiers et aux libertés (la fameuse loi de 1978, modifiée depuis) au profit du nouvel article 82 remplaçant le terme *« accord »* par celui de *« consentement »* tenant ainsi compte de la nouvelle terminologie consacrée par le RGPD.

Résultat, vis-à-vis de l'internaute : *« Ces accès* [à des informations déjà stockées dans son équipement terminal] *ou inscriptions* [des informations dans cet équipement] *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 »* (4). Le 21 mars 2019, l'avocat général de la Cour de justice de l'Union européenne (CJUE) présentait, dans l'affaire « Planet49 » des conclusions répondant à plusieurs questions préjudicielles posées par la cour fédérale de justice allemande sur l'encadrement du recours aux cookies et l'application du RGPD. L'avocat général rappelle notamment que pour être valide le consentement doit être *« éclairé »*. Cela implique que l'internaute doit être informé de la durée de fonctionnement des cookies, ainsi que de l'identité des tiers qui ont accès à ses informations par ce biais (5). Cette position est conforme aux recommandations du groupe de travail « Article 29 », devenu le Comité européen de la protection des données (CEPD), qui place le consentement au cœur du régime des données personnelles. Le CEPD précise que *« la notion de consentement telle que présentée dans le projet de règlement "ePrivacy" reste liée à la notion de consentement au sens du RGPD »* (6).

Prenant acte de ces évolutions et dans la continuité de son plan d'action 2019-2020 sur le ciblage publicitaire en ligne, publié en juin dernier, la Cnil a fait évoluer ses recommandations, anticipant elle aussi les évolutions du futur règlement « ePrivacy » qui remplacera la directive de 2002 et dont la dernière version du projet officiel a été publiée le 22 février dernier (7). L'autorité de contrôle française a ainsi adopté le 4 juillet dernier une délibération afin de remplacer les lignes directrices promulguées par la délibération de 2013 encadrant jusqu'à présent l'utilisation des cookies (8).

Elle montre sa volonté de faire du renforcement de l'encadrement du ciblage publicitaire une priorité et de mettre fin à des pratiques encore très répandues dans ce secteur. Ces nouvelles lignes directrices permettent ainsi d'apporter de premières explications sur l'application concrète du nouvel article 82 de la loi « Informatique et Libertés » (9).

Cookies « http », cookies « flash », etc.

Il ne s'agit que d'une première étape, puisque la Cnil a déjà annoncé qu'elle publierait d'autres recommandations sectorielles, notamment *« au premier trimestre 2020 »* une recommandation qui *« précisera les modalités pratiques de recueil du consentement »* (10), lesquelles feront suite à une consultation publique et une concertation avec les professionnels du secteur. *« Des groupes de travail se*

Notes

(1) - Directive 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

(2) - Directive 2009/136/CE du 25 novembre 2009 : http://lc.cx/ePrivacy

(3) - Proposition de règlement européen concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE.

tiendront au second semestre 2019 entre les services de la Cnil et chaque catégorie d'acteurs (éditeurs de contenus, annonceurs, prestataires et intermédiaires de l'écosystème du marketing, représentants de la société civile), par l'intermédiaire de leurs organisations professionnelles représentatives » (11). La Cnil revoit sa position et renforce les règles applicables aux cookies et autres traceurs. Les nouvelles lignes directrices de 2019 apportent des changements majeurs par rapport à ses recommandations antérieures de 2013.

Révision et renforcement des règles

A titre préliminaire, l'autorité de contrôle prend soin de préciser que le champ d'application de cette délibération est très large, puisqu'elle vise tous types de terminaux – notamment, smartphones, ordinateurs, consoles de jeux – et porte non seulement sur (12) : les cookies dit « http » (« par lesquels ces actions sont le plus souvent réalisées ») mais également sur les cookies dit « flash » (« local shared objects », ou objets locaux partagés), le « local storage » (ou stockage local) mis en œuvre au sein du HTML5, les identifications par calcul d'empreinte du terminal, les identifiants générés par les systèmes d'exploitation (qu'ils soient publicitaires ou non) et les identifiants matériels (adresses MAC, numéros de série, ...).

La Cnil réitère le principe selon lequel le consentement doit être manifesté par l'utilisateur « *de manière libre, spécifique, éclairée et univoque par une déclaration ou par un acte positif* » (13), conformément aux dispositions du RGPD (Article 7 concernant « les conditions applicables au consentement » du RGPD). L'autorité de contrôle française détaille les contours de ce principe par des illustrations. Ainsi, elle affirme sans ambiguïté que les « *cookies walls* », à savoir la pratique consistant à bloquer l'accès à un site Internet ou un service pour « *qui ne consent à être suivi* » est contraire à l'exigence d'un consentement libre.

De même, le consentement doit être spécifique, ce qui signifie que l'acceptation globale de conditions générales d'utilisation « *ne peut être une modalité valable de recueil du consentement* » qui doit être donné de manière distincte pour chaque finalité. Un simple renvoi vers des conditions générales d'utilisation ne saurait non plus suffire à répondre à l'exigence d'un consentement « *éclairé* » qui requiert qu'une information complète, visible, accessible et aisément compréhensible soit mise à disposition de l'utilisateur au moment du recueil de son consentement.

Enfin, l'un des changements les plus contraignants pour les acteurs du secteur de la publicité en ligne reste la suppression de la pratique dite du « *soft opt-in* », consacrée par la Cnil en 2013, consistant à considérer que la poursuite de la navigation sur un site Internet ou une application mobile valait consentement. Le caractère « univoque » du consentement requis par le RGPD exige à présent que l'internaute procède à une action positive pour recueillir son accord. Il ne sera plus non plus possible de se référer aux paramètres du navigateur de l'internaute, puisque la Cnil considère, conformément à la jurisprudence du Conseil d'Etat (14) que les « *nombreux réglages* » mis à disposition par les navigateurs web ne « *permettent pas d'assurer un niveau suffisant d'information préalable des personnes* », ni de « *distinguer les cookies en fonction de leurs finalités* ».

L'ensemble des exigences ne visent, néanmoins, que les cookies et traceurs pour lesquels un consentement est requis. De fait, la Cnil a réaffirmé le principe d'exemption pour certains cookies, notamment ceux dédiés aux mesures d'audience ou ceux destinés à « *permettre ou faciliter la communication par voie électronique* » ou « *strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* » (par exemple, les cookies d'identification).

Mais cette exception confirme la règle : continuer sa navigation ou *scroller*, autrement dit, faire défiler la page vers le bas de l'écran à l'aide de la molette d'une souris, d'un pavé tactile, mais également sur un écran tactile de téléphone portable ou de tablette à l'aide d'un doigt, n'est plus suffisant pour recueillir le consentement de l'internaute. Il faudra entreprendre les changements nécessaires pour assurer d'isoler le consentement de l'internaute et de rendre visibles les informations exigées. La preuve d'avoir recueilli, de manière conforme, le consentement de l'utilisateur, devra en outre être apportée et conservées par ses acteurs, lesquels devront pour ce faire mettre en place certainement de nouveaux outils, comme ceux d'historisation.

Délai accordé d'environ un an

Il est à noter que pour les opérateurs en conformité avec la délibération de 2013, la Cnil a concédé une période transitoire d'adaptation d'un an environ (six mois après la publication de la future recommandation prévue en 2020), laissant ainsi à ceux-ci le temps de mettre en œuvre les mesures opérationnelles qui s'imposent. Mais l'autorité a déjà prévenu que « *cette période d'adaptation n'empêchera pas la Cnil de contrôler pleinement le respect des autres obligations qui n'ont fait l'objet d'aucune modification et, le cas échéant, d'adopter des mesures correctrices pour protéger la vie privée des internautes* ». @

Notes

(4) - https://lc.cx/Article82

(5) - Conclusions de l'avocat général : https://lc.cx/Affaire C 673-17

(6) - https://lc.cx/LD-Consent10-04-18

(7) - https://lc.cx/ePrivacy15-02-19

(8) - Délibération n° 2013-378 du 5 décembre 2013.

(9) - Loi « Informatique et Libertés » n°78-17, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

(10) - Communiqué https://lc.cx/Cnil18-07-19

(11) - Communiqué https://lc.cx/Cnil28-06-19

(12) - Délibération n° 2019-093 du 4 juillet 2019, article 1.

(13) - Délibération n° 2019-093 du 4 juillet 2019, article 2.

(14) - Conseil d'Etat, 10e - 9e ch. réunies, décision du 6 juin 2018.