Consultation publique sur le projet de recommandation « cookies et autres traceurs »

Synthèse des contributions

Le 14 janvier 2020, la CNIL a lancé une consultation publique sur son projet de recommandation « cookies et autres traceurs » afin de recueillir les difficultés d'interprétation suscitées par le texte et des exemples de bonnes pratiques. Les contributions ont nourri les travaux de la CNIL en vue de la publication de la version définitive de sa recommandation.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Synthèse des contributions de la consultation publique sur le projet de recommandation « cookies et autres traceurs »

Cette consultation publique a fait l'objet de nombreuses contributions, tant du grand public que d'organismes privés et publics, tous concernés par les travaux de la CNIL sur le sujet des « cookies et autres traceurs ». La CNIL propose ici une synthèse des contributions les plus récurrentes.

À propos de la consultation publique de la CNIL sur son projet de recommandation « cookies et autres traceurs »

Le 4 juillet 2019, la CNIL publiait des lignes directrices sur l'application de l'article 82 de la loi Informatique et Libertés. Cet article encadre les actions visant à accéder ou à inscrire des informations dans le terminal d'un utilisateur, c'est-à-dire notamment le dépôt ou la lecture de cookies ou d'autres traceurs lorsque l'internaute se rend sur un site internet. Ces traceurs peuvent, par exemple, servir à adresser de la publicité ciblée, à personnaliser le contenu éditorial proposé à l'utilisateur ou encore à interagir avec des réseaux sociaux. Lorsqu'ils ne sont pas strictement nécessaires au fonctionnement du site visité, ces cookies ne peuvent être déposés qu'avec le consentement de l'utilisateur.

Dans le cadre de son plan d'action sur le ciblage publicitaire, la CNIL a conduit une concertation pendant l'automne 2019, afin d'élaborer un projet de recommandation proposant des modalités opérationnelles de recueil du consentement.

Ce projet a fait l'objet d'une consultation publique entre le 14 janvier et le 25 février 2020, en vue de la préparation de la version définitive de la recommandation.

Quelques chiffres

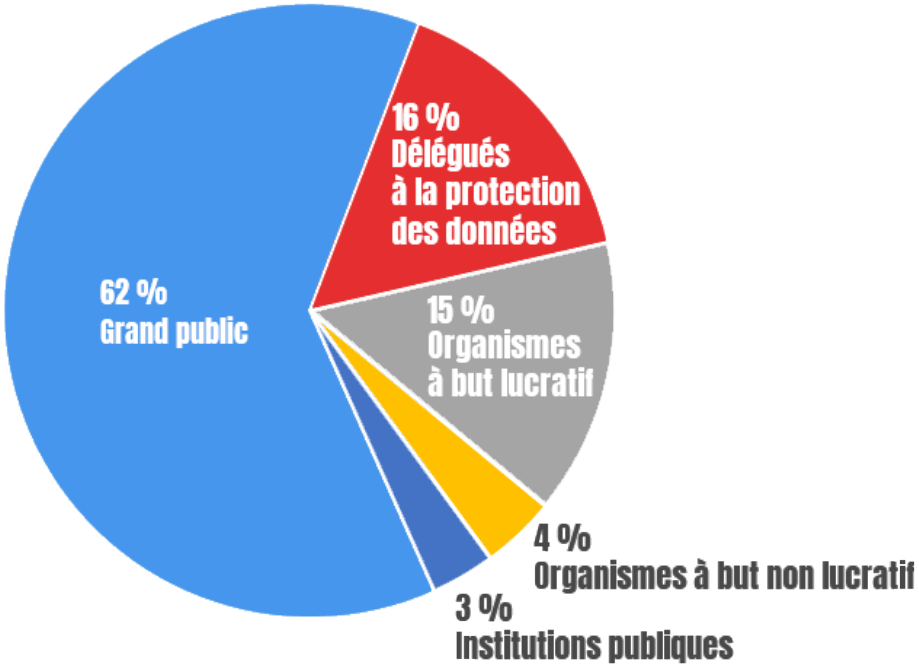
762
contributeurs

462
contributions écrites

4743
votes

462 contributions écrites et 4743 votes ont été adressés par 762 contributeurs :

- **476** contributeurs ont déclaré appartenir à la catégorie **« citoyens »** ;
- **119 délégués à la protection des données (DPD/DPO)** ou associations de délégués ;
- **111 organismes à but lucratif** dans des secteurs divers (presse, audiovisuel, e-commerce, etc.)
- **30 organismes à but non lucratif** ;
- **26 institutions publiques**.



Ces contributions ont permis à la CNIL :

- de faire évoluer, sur le fond et sur la forme, le projet de recommandation et les lignes directrices sur les « cookies et autres traceurs », afin d'y apporter certaines clarifications ;
- d'apporter des réponses, dans la synthèse ci-dessous ainsi que dans des FAQ dédiées, aux préoccupations les plus fréquemment partagées par les professionnels et le grand public lors de la consultation.

Sur les technologies concernées par la recommandation

Synthèse des contributions

De nombreux contributeurs se sont interrogés sur l'application de la recommandation à d'autres technologies que les seuls cookies web. Ces interrogations s'inscrivent dans un contexte où de nombreux navigateurs ont annoncé mettre en œuvre des mesures afin de restreindre l'usage de cookies déposés par des tiers et où les utilisateurs craignent que de nouvelles techniques de suivi de leur navigation soient mises en œuvre sans garanties pour les personnes concernées.

Témoignages de contributeurs

« Parler de cookies pour désigner le tracking des visiteurs porte à confusion et est risqué. On peut en effet identifier un navigateur par d'autres moyens. Par exemple, le *local storage* peut être utilisé pour suivre des visiteurs sur un site. Or, si on laisse penser aux gens que seuls les cookies peuvent être utilisés pour les traquer ou pire si l'on écrit qu'il faut le consentement uniquement pour les cookies les éditeurs peu scrupuleux en profiteront ».

« La technologie des cookies semble un peu dépassée pour certains autres façons de « *tracker* » les personnes développées, impossible à voir pour l'utilisateur (…) »

Éléments de réponse de la CNIL

La CNIL rappelle que le champ d'application de la recommandation ainsi que des lignes directrices est celui défini par la loi, qui vise toutes les opérations de lecture ou écriture réalisées dans le terminal de communication électronique d'un utilisateur d'un réseau de télécommunication ouvert au public.

Ainsi, la recommandation de la CNIL n'est pas limitée à l'usage des « cookies » ; elle a pour objectif d'aider les professionnels concernés dans leur démarche de mise en conformité **dès lors que ces derniers ont recours à des technologies qui nécessitent d'accéder à des informations déjà stockées ou à inscrire des informations dans l'équipement terminal de l'utilisateur** (« cookies Flash », « *local storage* », identification par calcul d'empreinte du terminal, identifiants générés par les systèmes d'exploitation, identifiants matériels, identifiant publicitaire, etc.).

Sur les traceurs qui ne nécessitent pas le consentement de l'utilisateur

Synthèse des contributions

De nombreux contributeurs considèrent que certains traceurs devraient être exemptés de consentement. Les contributions évoquent notamment :

- les traceurs utilisés pour personnaliser le contenu éditorial d'un service ;
- les traceurs servant à la facturation et à la mesure de la performance publicitaire (cookies dits de « *capping* », lutte contre la fraude au clic, etc.) utilisés notamment dans le cadre de la publicité contextuelle ;
- les traceurs utilisés pour la facturation des opérations d'affiliation ;
- les traceurs utilisés dans le cadre de la lutte contre la fraude et de la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT).
- les traceurs utilisés pour assurer la sécurité du dispositif d'authentification.

Éléments de réponse de la CNIL

La CNIL rappelle que les dispositions de l'article 82 de la loi Informatique et Libertés imposent le recueil du consentement avant toute action visant à stocker des informations ou à accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur, en dehors des exceptions prévues par ce même texte. Ainsi ces opérations sont exemptées de consentements dès lors qu'elles :

- ont pour finalité exclusive de permettre ou faciliter la communication par voie électronique (par exemple, la capacité d'acheminer l'information sur le réseau, la capacité d'échanger les données dans leur ordre prévu, la capacité de détecter les erreurs de transmission ou les pertes de données, etc.) ;
- sont strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Or, les quatre premiers traceurs évoqués ci-dessus n'ont pas vocation à faciliter une communication électronique et ne sont pas non plus strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur[1].

En revanche, comme souligné dans certaines contributions, les traceurs qui servent à identifier des tentatives de connections frauduleuses ou répétées dans le but de protéger le système de connexion contre les utilisations abusives sont exemptés de consentement, conformément aux exceptions prévues par l'article 82 de la loi Informatique et Libertés**. La CNIL a donc ajouté ces traceurs à la liste (non exhaustive) des traceurs qui, en l'état des pratiques portées à la connaissance de la CNIL, peuvent entrer dans l'une des exceptions ci-dessus mentionnées.** Cette liste est désormais intégrée dans les lignes directrices « cookies et autres traceurs » (ces traceurs étaient précédemment listés dans le projet de recommandation).

[1] Le fait qu'un traceur soit nécessaire à la viabilité économique du service n'implique pas qu'il soit « strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur » (Conseil d'État, 10ème - 9ème chambres réunies, 06/06/2018, 412589, Publié au recueil Lebon).

Sur la nécessité de permettre aux utilisateurs de refuser le dépôt de traceurs

Synthèse des contributions

Le projet publié pour consultation contenait des recommandations sur les modalités de mise en œuvre des possibilités de refus de l'utilisateur en préconisant l'intégration d'un bouton de refus placé au même niveau et dans les mêmes formes que celui ou ceux permettant de consentir, ce qui a fait l'objet de réactions très variables de la part des divers contributeurs. Si certains ont accueilli très favorablement ces recommandations, d'autres craignaient d'y voir une nouvelle obligation qui dépasserait ce que les textes exigent.

Éléments de réponse de la CNIL

Tout site qui dépose des traceurs doit proposer à l'utilisateur un moyen de les refuser avec la même simplicité que celui permettant de donner son consentement. Afin de répondre aux interrogations relatives aux modalités d'expression du refus, la CNIL a synthétisé, dans sa FAQ dédiée aux cookies et autres traceurs, les éléments présents dans ses lignes directrices et sa recommandation.

Sur la liste des responsables du traitement

Synthèse des contributions

Certains contributeurs se sont interrogés sur l'opportunité de faire figurer, lors du recueil du consentement, l'identité des responsables du traitement déposant des traceurs sur le terminal de l'utilisateur. Ces contributeurs ont mis en avant les difficultés pratiques que cela pouvait engendrer (notamment au regard du caractère rapidement évolutif d'une telle liste) et considèrent que cela ne participe pas à l'amélioration de l'information délivrée à l'utilisateur.

Témoignages de contributeurs

« Cette exigence de mise à jour est chronophage et exige la mobilisation de ressources et des investissements importants. La charge financière générée par cette obligation d'information sera lourde de conséquences pour les petites entités. En outre, pour effectuer cette mise à jour en temps réel et de manière permanente, les responsables de traitement devront s'assurer de l'exhaustivité de la liste, de son maintien à jour en continu et de son accessibilité à tout instant par les utilisateurs. »

« Au regard des difficultés évoquées pour disposer d'une liste exhaustive et mise à jour en continu des sociétés qui utilisent les cookies et autres traceurs, il semble plus pertinent de les regrouper par catégories. »

« Pour ce qui est de la liste exhaustive des responsables de traitement utilisant des traceurs sur le site ou l'application en temps réel, les éditeurs de sites ne la connaissent pas. En effet, les éditeurs connaissent les régies publicitaires avec lesquelles ils travaillent, mais ils ne connaissent pas nécessairement l'identité des annonceurs qui achètent les espaces publicitaires auxdites régies. »

Éléments de réponse de la CNIL

La CNIL rappelle que le caractère éclairé du consentement implique que l'utilisateur soit en mesure de pouvoir prendre connaissance de l'identité de l'ensemble des responsables du ou des traitements avant de pouvoir donner son consentement ou refuser. Pour simplifier, l'utilisateur doit connaître l'identité des organismes auxquels il donne son consentement. Cette obligation a également été rappelée par le Conseil d'Etat dans sa décision relative aux lignes directrices « cookies et autres traceurs » de la CNIL[2].

Dans sa recommandation du 17 septembre 2020, la CNIL rappelle qu'il est possible de faire figurer cette liste sur un second niveau d'information accessible depuis le premier écran (par exemple, via un lien hypertexte) afin

[2] Conseil d'État, 10ème - 9ème chambres réunies, 19/06/2020, 434684

de concilier cette obligation avec les exigences de clarté et de concision des informations eu égard aux contraintes d'ergonomie auxquelles sont confrontés les responsables du traitement.

Elle recommande également qu'une telle liste soit mise à la disposition des utilisateurs de manière permanente, à un endroit aisément accessible à tout moment sur le site web ou l'application mobile (par exemple, *via* un module de paramétrage accessible sur toutes les pages du site au moyen d'une icône statique toujours visible « cookie »).

Sur une approche européenne commune du sujet « cookies et autres traceurs »

Synthèse des contributions

Un certain nombre de contributions soulignent l'importance d'une harmonisation européenne sur ce sujet en soulignant les difficultés que pourraient poser d'éventuelles divergences d'interprétations :

- pour les opérateurs dont la mise en conformité serait complexifiée alors que ceux-ci opèrent dans un marché par nature européen, sinon international.
- pour les utilisateurs qui supporteraient les conséquences d'une telle complexité ; les règles seraient, selon divers contributeurs, mieux respectées si celles-ci s'appliquaient de manière uniforme au sein du territoire de l'Union.

Par ailleurs, certains contributeurs ont regretté la publication du projet de recommandation de la CNIL alors que la directive « ePrivacy », que l'article 82 de la loi « Informatique et Libertés » transpose en partie, fait actuellement l'objet de discussions dans le cadre d'une proposition de règlement déposée par la Commission européenne en janvier 2017.

Témoignages de contributeurs

« La CNIL devrait chercher à atteindre une harmonisation maximale avec les autres autorités européennes de protection des données en ce qui concerne l'interprétation et l'application des dispositions du RGPD (EU 2016/679) relatives au consentement. »

« Le [nom du contributeur] considère que la recommandation anticipe le projet de règlement ePrivacy, ce qui va au-delà des pouvoirs de la CNIL. »

Éléments de réponse de la CNIL

Pour rappel :

- les dispositions relatives aux traceurs découlent d'une directive (la directive 2002/58/CE dite « ePrivacy ») dont les transpositions nationales peuvent, dans une certaine mesure, varier au sein de chaque Etat-membre ;
- les autorités de protection des données ne sont pas systématiquement compétentes, au niveau national, pour faire appliquer ces transpositions nationales[3] ;
- seul le règlement ePrivacy pourra garantir un haut niveau d'uniformisation entre les Etats membres ;

Pour autant, la CNIL rappelle que l**es autorités de protection des données compétentes sur les transpositions nationales d' « ePrivacy » échangent régulièrement sur ces questions. Ces échanges, formels et informels, contribuent à harmoniser, dans la mesure du possible, les positions européennes sur le sujet.**

S'agissant de la révision de la directive « ePrivacy », la CNIL apporte des éléments de réponse dans sa FAQ.

[3] En effet, la directive « ePrivacy » laisse aux Etats membres la responsabilité de désigner la ou les autorités compétentes pour l'application des dispositions transposant la directive.

Sur les designs manipulateurs (« *dark patterns* »)

Synthèse des contributions

De nombreux contributeurs ont souhaité s'exprimer sur les enjeux de design évoqués dans le projet de recommandation publié pour consultation. Certaines contributions mettent en avant des exemples de pratiques qu'ils jugent trompeuses, voire « déloyales », alors que d'autres défendent le droit de l'éditeur à convaincre l'utilisateur d'accepter les cookies, y compris à travers une grammaire visuelle spécifiquement élaborée pour l'y inciter.

Témoignages de contributeurs

« [Une signalétique non standardisée] rendrait plus difficile pour les entreprises mal intentionnées de faire des *popups* imbitables pleines de textes indéchiffrables. Si on le fait sur les produits transformés comme par exemple les plats alors que les gens sont censés savoir ce dont il s'agit, cela aura d'autant plus d'intérêt dans un domaine qui reste flou ou obscur pour la majorité des gens. »

« Dès lors que l'éditeur veille à ne pas réaliser de communication trompeuse, à respecter les principes de loyauté, de simplicité dans l'accès au paramétrage et d'exhaustivité de l'information, le risque de de tromper l'internaute semble être écarté, quelle que soit la « grammaire visuelle » adoptée. »

« Certain tentent de dissuader les gens avec de nombreux clics, doubles négations, et autres méthodes fourbes. »

« Il suffit d'échantillonner le web d'aujourd'hui pour voir à quel point les éditeurs de mauvaise foi rivalisent d'imagination pour rendre le refus onéreux : renvois d'une page de configuration sur l'autre, parfois même sur d'autres sites, bouton de refus enterré au bas de longues listes, longues digressions hors-sujet [,] etc. »

« Retirer aux éditeurs une possibilité d'influer, même en toute bonne foi, c'est leur retirer tout moyen de lutter contre les aspects anxiogènes qui fait passer le cookie pour quelque chose de foncièrement mauvais, alors que ce sont ses utilisations détournées uniquement qui le sont. On ne demande pas à un constructeur automobile de diviser en deux ses pages de publicité pour lister tous les cas de pannes et d'accidents possibles avec le véhicule vendu… »

Éléments de réponse de la CNIL

La question des pratiques de design trompeuses (dites « *dark patterns* ») fait l'objet, ces dernières années, d'une attention particulière, y compris dans le domaine de la protection des données personnelles. Dans son cahier IP N° 6 *La forme des choix*, la CNIL a indiqué qu'il *« pourrait être considéré que le design abusif ou trompeur des services numériques peut engendrer divers troubles au consentement* », en particulier quant à son caractère libre, tout en précisant que la tromperie devrait être d'« *une nature suffisamment objective et démontrable pour qu'il entraine son invalidité* ».

La CNIL recommande que les responsables de traitement s'assurent que les interfaces de recueil des choix n'intègrent pas de pratiques de design potentiellement trompeuses, laissant penser aux utilisateurs que leur consentement est obligatoire ou qui mettent visuellement plus en valeur un choix plutôt qu'un autre.

Document de référence

- **La loi Informatique et libertés**
- **Les lignes directrices sur les cookies et autres traceurs**
- **La recommandation sur les cookies et autres traceurs**
- **Site web de la CNIL**