Rechercher dans le texte...

Réinitialiser

Version initiale

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 le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE ;
Vu la directive 2002/58/ CE 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 modifiée par la directive 2009/136/ CE du 25 novembre 2009 ;
Vu la directive 2008/63/ CE relative à la concurrence dans les marchés des équipements terminaux de télécommunications, notamment son article 1er ;
Vu la loi n° 78-17 du 6 janvier 1978modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-I-2° bet 82 ;
Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
Vu les lignes directrices sur le consentement au sens du règlement (UE) 2016/679 adoptées le 10 avril 2018 par le groupe de travail « de l'article 29 » sur la protection des données et endossées par le Comité européen de la protection des données (CEPD) le 25 mai 2018 ;
Vu la déclaration du 25 mai 2018 du Comité européen de la protection des données sur la révision de la directive « vie privée et communications électroniques » et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques ;
Vu l'avis 5/2019 sur la relation entre la directive « vie privée et communications électroniques » et le RGPD, concernant en particulier la compétence, les missions et pouvoirs des autorités de protection des données, adopté par le Comité européen de la protection des données (CEPD) le 12 mars 2019 ;
Vu la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978 ;

Article

Après avoir entendu M. François PELLEGRINI, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,
Adopte les lignes directrices suivantes :
La Commission nationale de l'informatique et des libertés (CNIL) est chargée de veiller au respect des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi Informatique et Libertés), ainsi que des autres textes relatifs à la protection des données à caractère personnel.
Les présentes lignes directrices ont pour objet de rappeler le droit applicable aux opérations de lecture ou écriture dans le terminal d'un utilisateur, et notamment l'usage des cookies et autres traceurs. Elles visent notamment des dispositions de la directive 2002/58/ CE modifiée «le privée et communications électroniques (ou «PrivacY) transposée en droit français à l'article 82 de la loi Informatique et Libertés, et la définition du consentement figurant à l'article 4 du règlement général sur la protection des données (RGPD) tel qu'interprété dans les lignes directrices du Comité européen de la protection des données (CEPD).
En cas de manquement à ces dispositions, la Commission rappelle qu'elle peut prendre toutes mesures correctives et sanctions vis-à-vis des organismes qui y sont soumis, en application de l'article 3 de la loi, et ce notamment de manière indépendante des dispositions du chapitre VII du RGPD en matière de coopération et de cohérence, dans la mesure où l'article 82 révoque de la transposition d'une directive distincte.
L'article 82 de la loi dispose que :
Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a déÀ 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.
Cet article, qui transpose l'article 5 (3) de la directive vie privée et communications électroniques, impose ainsi 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 applicables.
La Commission rappelle que les présentes lignes directrices ne concernent que la mise en œuvre des dispositions de l'article 82 de la loi Informatique et Libertés ; les éventuels traitements de données à caractère personnel utilisant les données collectées via les opérations de lecture ou écriture doivent, par ailleurs, respecter l'ensemble des dispositions légales applicables.
Le consentement prévu par ces dispositions doit être conforme à la définition et aux conditions prévues aux articles 4 (11) et 7 du RGPD.
Le RGPD exige renforcer les garanties en matière de consentement des personnes, en apportant des clarifications sur ses conditions d'obtention et sur la nécessité d'en démontrer le recueil.
Le renforcement des droits des personnes conduit la Commission à abroger sa délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978 (ci-après à recommandation cookies et autres traceurs) pour la remplacer par les présentes lignes directrices. Ces lignes directrices seront complétées ultérieurement par des recommandations sectorielles ayant notamment vocation à préciser les modalités pratiques du recueil du consentement.

Liens relatifs

Article 1

Sur le champ d'application des lignes directrices.
Les présentes lignes directrices s'appliquent à toutes les opérations visant à accéder, par voie de transmission électronique, à des informations déjà stockées dans le terminal de l'abonné ou de l'utilisateur ou à inscrire des informations dans cet équipement.
La Commission relève que l'article 1er de la directive 2002/58/CE définit l'équipement terminal comme tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations ; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique ; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public.
Cette définition englobe de nombreux dispositifs couramment utilisés, tels qu'une tablette, un mobile multifonction (smartphone), un ordinateur fixe ou mobile, une console de jeux vidéo, une télévision connectée, un véhicule connecté, un assistant vocal, ainsi que tout autre objet connecté à un réseau de télécommunication ouvert au public.
Les présentes lignes directrices s'appliquent quels que soient les systèmes d'exploitation, les logiciels applicatifs (tels que les navigateurs) ou les terminaux utilisés.
Les lignes directrices portent sur l'utilisation des cookies et TPP par lesquels ces actions sont le plus souvent réalisées, mais ont également vocation à s'appliquer au recours à d'autres techniques : les local shared objects (objets locaux partagés) appelés parfois les cookies Flash , le local storage (stockage local) mis en œuvre au sein du HTML 5, les identifications par calcul d'empreinte du terminal, les identifiants générés par les systèmes d'exploitation (qu'ils soient publicitaires ou non : IDFA, IDFV, Android ID, etc.), les identifiants matériels (adresse MAC, numéro de série ou tout autre identifiant d'un appareil), etc. Pour l'application des présentes lignes directrices, le mot traceur désignera l'ensemble des dispositifs visés par l'article 82 de la loi.
Le fait que les informations (stockées et/ou consultées) soient ou non des données à caractère personnel au sens du RGPD n'est pas une condition préalable à l'application de l'article 5, paragraphe 3 de la directive 2002/58/CE. Par conséquent, l'article 82 précité s'applique indépendamment du fait que les données concernées soient à caractère personnel ou non.
Enfin, la Commission attire l'attention des organismes concernés sur le fait que tout traitement portant sur un traceur, dès lors que celui-ci relève de la catégorie des données à caractère personnel - parfois directement identifiantes (par exemple, une adresse électronique) et souvent indirectement identifiantes (par exemple, l'identifiant unique d'un cookie, une adresse IP, un identifiant du terminal ou d'un composant du terminal de l'utilisateur, le résultat du calcul d'empreinte du terminal ou de tout autre traceur, ou encore un identifiant généré par un logiciel ou un système d'exploitation) - impose le respect des dispositions du RGPD.

Article 2

Sur les modalités de recueil du consentement
En application de la loi Informatique et Libertés , du RGPD et des lignes directrices du CEPD sur le consentement, les traceurs nécessitant un recueil du consentement ne peuvent être utilisés en écriture ou en lecture tant que l'utilisateur n'a pas préalablement manifesté à cette fin sa volonté, de manière libre, spécifique, éclairée et univoque par une déclaration ou par un acte positif clair.
S'agissant du caractère libre du consentement
La Commission considère que le consentement ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et ne subit pas d'inconvénients majeurs en cas d'absence ou de retrait de consentement.
A ce titre, la Commission rappelle que le CEPD, dans sa déclaration sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques , a considéré que la pratique qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à être suivi (cookie walls) n'est pas conforme au RGPD. Le CEPD considère en effet que, dans une telle hypothèse, les utilisateurs ne sont pas en mesure de refuser le recours à des traceurs sans subir des conséquences négatives (en l'occurrence l'impossibilité d'accéder au site consulté).
S'agissant du caractère spécifique du consentement
La Commission rappelle que la personne concernée doit être en mesure de donner son consentement de façon indépendante et spécifique pour chaque finalité distincte. Le fait d'offrir par ailleurs à la personne concernée la possibilité de consentir de manière globale est acceptable, à condition que cela s'ajoute, sans la remplacer, à la possibilité de consentir spécifiquement à chaque finalité.
A ce titre, l'acceptation globale de conditions générales d'utilisation ne peut être une modalité valable de recueil du consentement, dans la mesure où celui-ci ne pourra être donné de manière distincte pour chaque finalité.
S'agissant du caractère éclairé du consentement
La Commission rappelle que l'information doit être rédigée en des termes simples et compréhensibles pour tous, et qu'elle doit permettre aux utilisateurs d'être parfaitement informés des différentes finalités des traceurs utilisés. Elle considère que l'utilisation d'une terminologie juridique ou technique trop complexe ne répond pas à l'exigence d'information préalable.
La Commission rappelle que l'information doit être complète, visible, et mise en évidence au moment du recueil du consentement. Un simple renvoi vers les conditions générales d'utilisation ne saurait suffire.
Les informations devant être portées à la connaissance des utilisateurs, préalablement au recueil du consentement, en application de l'article 82, sont à minima :

- l'identité du ou des responsables de traitement ;
- la finalité des opérations de lecture ou écriture des données ;
- l'existence du droit de retirer son consentement.

Lorsqu'un traitement de données à caractère personnel suit l'opération de lecture ou écriture et que celui-ci est fondé sur le consentement, l'information préalable donnée aux utilisateurs doit être alors complétée afin de satisfaire aux exigences des lignes directrices du CEPD sur le consentement.
La Commission rappelle qu'afin que le consentement soit éclairé, l'utilisateur doit pouvoir identifier l'ensemble des entités ayant recours à des traceurs avant de pouvoir y consentir. Ainsi, la liste exhaustive et régulièrement mise à jour de ces entités doit être mise à disposition auprès de l'utilisateur directement lors du recueil de son consentement.
S'agissant du caractère univoque du consentement
La Commission souligne que le consentement doit se manifester par le biais d'une action positive de la personne préalablement informée des conséquences de son choix et disposant des moyens de l'exercer. Le fait de continuer à naviguer sur un site web, d'utiliser une application mobile ou bien de faire défiler la page d'un site web ou d'une application mobile ne constitue pas des actions positives claires assimilables à un consentement valable.
Elle considère également que l'utilisation de cases pré-cochées, tout comme l'acceptation globale de conditions générales d'utilisation, ne peuvent être considérées comme un acte positif clair visant à donner son consentement.
Des systèmes adaptés doivent donc être mis en place pour recueillir le consentement selon des modalités pratiques qui permettent aux utilisateurs de bénéficier de solutions conviviales et ergonomiques.
Sur la preuve du consentement
L'article 7 du RGPD impose que le consentement soit démontrable, ce qui signifie que les organismes exploitant des traceurs doivent mettre en œuvre des mécanismes leur permettant de démontrer, à tout moment, qu'ils ont valablement recueilli le consentement des utilisateurs. Dans la situation où ces organismes ne recueillent pas eux-mêmes le consentement des personnes, la Commission rappelle qu'une telle obligation ne saurait être remplie par la seule présence d'une clause contractuelle engageant l'une des organisations à recueillir un consentement valable pour le compte de l'autre partie.
Sur le retrait du consentement
La Commission rappelle qu'il doit être aussi facile de refuser ou de retirer son consentement que de donner. Cela signifie notamment que les personnes ayant donné leur consentement à l'utilisation de traceurs doivent être en mesure de le retirer à tout moment. Des solutions conviviales doivent donc être mises en œuvre pour que les personnes puissent retirer leur consentement aussi facilement qu'elles ont pu le donner.

Article 3

Sur les rôles et responsabilités des acteurs.
Les technologies concernées par l'obligation de recueil du consentement n'impliquent pas systématiquement de traitement de données à caractère personnel. Toutefois, dans un grand nombre de cas, les opérations de lecture ou écriture concernent des données à caractère personnel et feront partie intégrante d'un traitement de données à caractère personnel soumis aux autres dispositions de la loi et du RGPD, ce qui implique la nécessité de qualifier les parties concernées.
Si, dans un certain nombre de cas, l'utilisateur du traceur fait intervenir une seule entité qui est donc pleinement responsable de l'obligation de recueillir le consentement (par exemple un éditeur de site web qui a recours à des traceurs pour réaliser lui-même les statistiques d'usage de son service), dans d'autres cas, plusieurs acteurs contribuent à la réalisation des opérations de lecture ou écriture visées par les présentes lignes directrices (par exemple un éditeur de site web et une régie publicitaire déposant des cookies lors de la consultation du site web). Dans ce dernier cas, ces entités peuvent être considérées comme responsables de traitement uniques , responsables conjoints ou comme sous-traitants.
La Commission constate que, dans d'autres cas, les tiers ayant recours à des traceurs seront pleinement et indépendamment responsables des traceurs qu'ils mettent en œuvre, ce qui signifie qu'ils devront assumer indépendamment l'obligation de recueillir le consentement des utilisateurs.
Dans le cas d'une responsabilité conjointe, elle rappelle les responsables déterminent conjointement les finalités et les moyens du traitement. La Commission rappelle qu'aux termes de l'article 26 du RGPD, ils devront définir de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD, en particulier en ce qui concerne le recueil et la démonstration, le cas échéant, d'un consentement valable.
Enfin, en qualité de sous-traitant un acteur qui collecte des informations et/ou accède à des informations sur des traceurs dans l'équipement terminal d'un abonné ou d'un utilisateur, exclusivement pour le compte d'un responsable de traitement et sans réutilisation pour son propre compte des données collectées via le traceur. La Commission rappelle que si une relation de sous-traitance est établie, le responsable de traitement et le sous-traitant doivent établir un contrat ou un autre acte juridique précisant les obligations de chaque partie, dans le respect des dispositions de l'article 28 du RGPD.

Article 4

Sur les paramètres du terminal.
L'article 82 de la loi précise que le consentement peut résulter de paramètres appropriés du dispositif de connexion de la personne ou de tout autre dispositif placé sous son contrôle.
La Commission considère que ces paramètres du navigateur ne peuvent, en l'état de la technique, permettre à l'utilisateur d'exprimer la manifestation d'un consentement valide.
Tout d'abord, si les navigateurs web proposent de nombreux réglages permettant aux utilisateurs d'exprimer des choix en matière de cookies, force est de constater que ceux-ci sont exprimés dans des conditions ne permettant pas d'assurer un niveau suffisant d'information préalable des personnes.
Ensuite, quels que soient les mécanismes existants, les navigateurs ne permettent pas de distinguer les cookies en fonction de leurs finalités, ce qui signifie que l'utilisateur n'est pas non plus en mesure de consentir de manière spécifique pour chaque finalité.
Enfin, les paramètres du navigateur ne permettent pas aujourd'hui d'exprimer un choix sur d'autres technologies que les cookies (telle que le fingerprinting par exemple) à des fins de suivi de la navigation.
Toutefois, les navigateurs pourraient évoluer afin d'intégrer des mécanismes permettant de recueillir un consentement conforme au RGPD. La Commission considère qu'une telle évolution serait de nature à garantir, d'une part, que les internautes disposent d'outils efficaces et simples leur permettant de consentir de façon simple et, d'autre part, que les éditeurs qui ne disposent pas des moyens ou des compétences pour mettre en place des mécanismes de recueil du consentement puissent s'appuyer sur de tels mécanismes.

Article 5

Sur le cas spécifique des traceurs de mesure d'audience.
Un éditeur peut avoir besoin de mesurer l'audience de son site web ou de son application, ou bien de tester des versions différentes afin d'optimiser ses choix éditoriaux en fonction de leurs performances respectives. Des traceurs sont fréquemment utilisés pour cette finalité et ces dispositifs peuvent, dans certains cas, être regardés comme nécessaires à la fourniture du service explicitement demandé par l'utilisateur, sans présenter de caractère particulièrement intrusif pour ceux-ci, et ainsi être exemptés du recueil du consentement. Par exemple, les statistiques de fréquentation et les tests visant à mesurer les performances relatives de différentes versions d'un même site web (couramment appelés tests A/B) permettent notamment aux éditeurs de détecter des problèmes de navigation dans leur site ou leur application ou encore d'organiser les contenus.
Dès lors, la Commission considère que peuvent bénéficier de cette exemption au recueil du consentement, les traitements respectant les conditions suivantes :

- ils doivent être mis en œuvre par l'éditeur du site ou bien par son sous-traitant ;
- la personne doit être informée préalablement à leur mise en œuvre ;
- elle doit disposer de la faculté de s'y opposer par l'intermédiaire d'un mécanisme d'opposition facilement utilisable sur l'ensemble des terminaux, des systèmes d'exploitation, des applications et des navigateurs web. Aucune opération de lecture ou d'écriture ne doit avoir lieu sur le terminal depuis lequel la personne s'est opposée ;
- la finalité du dispositif doit être limitée à (i) la mesure d'audience du contenu visualisé afin de permettre l'évaluation des contenus publiés et l'ergonomie du site ou de l'application, (ii) la segmentation de l'audience du site web en cohortes afin d'évaluer l'efficacité des choix éditoriaux, sans que cela ne conduise à cibler une personne unique et (iii) la modification dynamique d'un site de façon globale. Les données à caractère personnel collectées ne doivent pas être recoupées avec d'autres traitements (fichiers clients ou statistiques de fréquentation d'autres sites, par exemple) ni transmises à des tiers. L'utilisation des traceurs doit également être strictement cantonnée à la production de statistiques anonymes. Sa portée doit être limitée à un seul éditeur de site ou d'application mobile et ne doit pas permettre le suivi de la navigation de la personne utilisant différentes applications ou naviguant sur différents sites web ;
- l'utilisation de l'adresse IP pour géolocaliser l'internaute ne doit pas fournir une information plus précise que la ville. L'adresse IP collectée doit également être supprimée ou anonymisée une fois la géolocalisation effectuée ;
- les traceurs utilisés par ces traitements ne doivent pas avoir une durée de vie excédant trèze mois et cette durée ne doit pas être prorogée automatiquement lors des nouvelles visites. Les informations collectées par l'intermédiaire des traceurs doivent être conservées pendant une durée de vingt-cinq mois maximum.

Article 6

Sur les opérations de lecture ou écriture non soumises au consentement préalable.
L'article 82 prévoit que l'exigence du consentement préalable ne s'applique pas 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 :

- a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; ou
- est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Article 7

Abrogation de la recommandation n° 2013-378 du 5 décembre 2013.

Liens relatifs

Article

La présente délibération abroge la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.
La présente délibération sera publiée au Journal officiel de la République française.

Liens relatifs

La présidente,
M.-L. Denis

Extrait du Journal officiel électronique authentifié
PDF - 237,7 Ko