GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

14/FR
WP 224

Avis 9/2014 sur l'application de la directive 2002/58/CE à la capture d'empreintes numériques

Adopté le 25 novembre 2014

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale «Justice» de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

1. Résumé

La capture d'empreintes numériques pose de graves problèmes pour la protection des données des personnes physiques. Ainsi, plusieurs services en ligne ont proposé la capture d'empreintes numériques comme une solution de rechange aux cookies HTTP à des fins analytiques ou de pistage qui permettrait d'échapper à l'obligation de consentement visée à l'article 5, paragraphe 3[1]. Cela prouve que les risques présentés par la capture d'empreintes ne sont nullement théoriques, et des études montrent que cette technique est d'ores et déjà exploitée[2].

Dans le présent avis, le groupe de travail «Article 29» (GT29) se penche sur la question de la capture d'empreintes numériques et sur l'applicabilité de l'article 5, paragraphe 3, de la directive 2002/58/CE «vie privée et communications électroniques», modifiée par la directive 2009/136/CE, sans préjudice des dispositions de la directive 95/46/CE sur la protection des données. Le message clé de l'avis est que l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique à la capture d'empreintes numériques.

Le présent avis complète l'avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies[3] et indique aux tiers[4] qui traitent des empreintes numériques générées par l'obtention de l'accès à des informations ou le stockage d'informations dans l'équipement terminal de l'utilisateur qu'ils ne peuvent le faire qu'avec le consentement valable de ce dernier (à moins qu'une exemption ne s'applique).

2. Introduction

Aux termes de l'article 5, paragraphe 3, de la directive 2002/58/CE (directive «vie privée et communications électroniques»), modifiée par la directive 2009/136/CE[5], les États membres garantissent que «*le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur*» n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE[6] (directive sur la protection des données), une information claire et complète, entre autres sur les finalités du traitement[7].

---

[1] *Wall Street Journal*, 2013. «Web Giants Threaten End to Cookie Tracking». http://online.wsj.com/news/articles/SB10001424052702304682504579157780178992984

[2] Nikiforakis, 2013. *Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting*. https://lirias.kuleuven.be/bitstream/123456789/393661/1/

[3] Groupe de travail «Article 29», 2012. Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf

[4] «Tiers» tel que visé au considérant 66 de la directive 2009/136/CE.

[5] http://eur-lex.europa.eu/legal-content/fr/ALL/?uri=CELEX:32009L0136

[6] http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:31995L0046

[7] Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement

Dans son avis 04/2012, le GT29 se penche sur l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» dans le cadre du stockage d'informations, ou de l'accès à des informations, au moyen de cookies. Il y précise que ledit article ne s'applique pas exclusivement aux cookies, mais aussi aux «technologies similaires».

Le présent avis tire les conséquences de ce que, selon des informations toujours plus nombreuses, des tiers s'emploient activement à explorer des technologies de remplacement des cookies à des fins diverses, dans l'idée de contourner l'obligation de consentement prévue à l'article 5, paragraphe 3. En particulier, il examine la technique dite de «capture d'empreintes numériques», c'est-à-dire la combinaison d'un ensemble d'éléments d'information visant à identifier de manière univoque un appareil particulier ou une instance d'application.

Les empreintes numériques peuvent aussi constituer des données à caractère personnel. Si le présent avis ne procède pas à une analyse des dispositions applicables de la directive sur la protection des données, il n'en fait pas moins référence à des questions de protection des données qui sont particulièrement pertinentes dans le contexte de la capture d'empreintes numériques. Par exemple, lorsque plusieurs éléments d'information sont reliés, notamment des identifiants uniques tels qu'une adresse IP, et que la finalité du traitement consiste à identifier les utilisateurs dans la durée et d'un site web à l'autre, comme dans la publicité comportementale. En pareil cas, le traitement est soumis également aux règles de la directive sur la protection des données.

La technologie de la capture d'empreintes numériques ne se limite pas aux paramètres de configuration d'un navigateur web classique sur un ordinateur de bureau. Elle n'est pas non plus assujettie à un protocole particulier, mais peut s'utiliser pour capter l'empreinte numérique d'un vaste ensemble d'équipements, de produits électroniques grand public et d'applications connectés à l'internet, dont les applications tournant sur des appareils mobiles, des téléviseurs intelligents, des consoles de jeux, des lecteurs de livres numériques, des radios internet, des systèmes embarqués automobiles ou des compteurs intelligents[8].

3. Définition

Le document RFC6973[9] définit l'empreinte numérique comme étant «un ensemble d'éléments d'information qui identifient un appareil ou une instance d'application». Le présent avis emploie le terme en un sens large, comme désignant tout ensemble d'informations pouvant être utilisé pour identifier un utilisateur, un agent utilisateur ou un appareil dans la durée par un procédé d'individualisation[10], de corrélation[11] ou d'inférence[12]. Cela comprend, entre autres, les données tirées:

---

nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

[8] Ces ensembles connectés sont parfois désignés sous le terme d'«internet des objets».

[9] Cooper, 2013. *Privacy Considerations for Internet Protocols*. http://tools.ietf.org/html/rfc6973

[10] *Individualisation*: possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données, Avis 05/2014 sur les techniques d'anonymisation, p. 13.

[11] *Corrélation*: capacité de relier entre eux au moins deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases

a) de la configuration d'un agent utilisateur ou d'un appareil, ou

b) de données exposées par l'usage de protocoles de communication de réseau.

Les données susceptibles de former une empreinte numérique sont nombreuses, et la liste qui suit ne prétend pas être exhaustive:

a) informations CSS;

b) objets JavaScript (p. ex., document, fenêtre, écran, navigateur, date et langue);

c) informations d'en-tête HTTP (p. ex., nombre de bits d'information de la chaîne «agent utilisateur», ordonnancement des en-têtes HTTP, variante d'en-tête HTTP par type de requête);

d) informations d'horloge (p. ex., décalage d'horloge et erreur d'horloge);

e) implémentation de pile TCP;

f) polices installées;

g) informations sur les modules d'extension installés (p. ex., informations de configuration et de version)[13];

h) utilisation d'interfaces de programmation applicative (API) internes[14] exposées par l'agent utilisateur ou l'appareil;

i) utilisation d'API externes des services internet avec lesquels l'agent utilisateur ou l'appareil est en train de communiquer.

4. Contexte technique

L'internet et la toile ont été conçus en pensant aux besoins d'un environnement de réseau résilient, à architecture ouverte[15]. Du fait des choix de conception opérés pour répondre à ces besoins, les appareils transmettent des éléments d'information. Un ensemble de protocoles comprennent une série d'éléments d'information obligatoires et facultatifs. Par exemple, le protocole HTTP/1.1[16] spécifie des

---

de données différentes). Si une attaque permet d'établir (par exemple, au moyen d'une analyse de corrélation) que deux enregistrements correspondent à un même groupe d'individus, mais ne permet pas d'isoler des individus au sein de ce groupe, la technique résiste à l'«individualisation», mais non à la corrélation, Avis 05/2014 sur les techniques d'anonymisation, p. 13.

[12] *Inférence*: possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs, Avis 05/2014 sur les techniques d'anonymisation, p. 13.

[13] Voir a) http://www.w3.org/wiki/Fingerprinting, b) http://w3c.github.io/fingerprinting-guidance/#wsj-orbitz, c) https://wiki.mozilla.org/Fingerprinting et d) https://trac.webkit.org/wiki/Fingerprinting for mechanisms.

[14] L'API offre un cadre facile d'utilisation pour accéder à des fonctions ou à des sous-programmes au sein d'un composant logiciel.

[15] Kahn, 1972. *Communications Principles for Operating Systems*. Note interne de BBN.

[16] Fielding, Reschke, 2014. *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*. http://www.ietf.org/rfc/rfc7231.txt

champs d'en-tête permettant au serveur et au client d'inclure des informations complémentaires sur l'hypertexte. Certains de ces champs servent expressément à la reconnaissance de types de clients par le serveur. Par exemple, le champ de l'en-tête de requête «agent utilisateur» comporte la description suivante: «*Cette information est utilisée à des fins statistiques, pour le pistage des violations de protocole et pour la reconnaissance automatique des agents utilisateurs, dans le souci d'adapter la réponse à l'agent et d'éviter ainsi que des agents particuliers ne soient pénalisés*».

La chaîne «agent utilisateur» est généralement utilisée pour optimiser la présentation du contenu en fonction de l'appareil concerné, cibler des utilisateurs spécifiques[17] ou recueillir des informations sur l'appareil à des fins de sécurité ou de suivi analytique.

5. Risques pour la protection des données

Un en-tête HTTP n'ayant généralement pas de valeur unique, il est rare qu'un utilisateur puisse être identifié au moyen de ce seul élément d'information[18]. Par exemple, les types de médias pris en charge par un navigateur sont souvent les mêmes pour les utilisateurs qui partagent la même version du navigateur. De ce fait, lorsqu'ils sont traités de manière isolée, ces éléments d'information non univoques ne présentent généralement pas de risques pour la protection des données.

Toutefois, plusieurs éléments d'information peuvent être combinés de manière à former un ensemble suffisamment univoque (en particulier lorsqu'ils sont combinés avec d'autres identificateurs comme l'adresse IP émettrice) pour faire office d'empreinte numérique unique de l'appareil ou de l'instance d'application. Une telle empreinte numérique permet de distinguer les appareils entre eux et peut être utilisée comme une solution subreptice de rechange aux cookies pour le pistage du comportement des internautes dans la durée[19], [20], [21]. Par voie de conséquence, une personne peut être associée à cette empreinte numérique, et donc être identifiée ou rendue identifiable par celle-ci.

Les risques posés par la capture d'empreintes numériques en matière de protection des données sont encore aggravés par le fait que l'ensemble univoque d'éléments d'information n'est pas seulement accessible à l'éditeur du site web, mais à beaucoup d'autres tiers. Cette situation, qui contraste totalement avec la politique de la *même origine* régissant les cookies HTTP, est exacerbée par la spécificité technique de la toile mondiale, où de nombreux tiers contribuent au contenu d'une page web.

Il est courant qu'une page web soit générée de façon dynamique, en temps réel, à partir des contenus renvoyés par de multiples sources. Chacune de ces ressources va générer ses propres requêtes HTTP et

[17] Wall Street Journal, 2012. «On Orbitz, Mac Users Steered to Pricier Hotels». http://www.wsj.com/articles/SB10001424052702304458604577488822667325882

[18] Il arrive qu'un élément d'information contienne à lui seul des informations susceptibles d'identifier de manière univoque une personne; c'est le cas, par exemple, du jeton d'accès OAuth.

[19] Panopticlick, Electronic Frontier Foundation, 2010. https://panopticlick.eff.org/

[20] Yen, 2012. *Host Fingerprinting and Tracking on the Web: Privacy and Security Implications*. http://research.microsoft.com/pubs/156901/ndss2012.pdf

[21] Eckersley, 2010. *A Primer on Information Theory and Privacy*. https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

télécharger des images et des fichiers JavaScript et CSS. D'autre part, beaucoup de pages web contiennent des pixels espions et des scripts de pistage. Elles peuvent aussi émettre des requêtes HTTP qui enregistrent les événements d'interaction de l'utilisateur avec la page (défilement, clic sur une page, une image ou une publicité). Il est donc souvent possible à des tiers de recueillir les informations nécessaires pour capturer l'empreinte numérique de l'appareil de l'utilisateur.

Les risques pour la protection des données ne se limitent pas au pistage par des tiers. La combinaison des données obtenues par le moyen des interfaces de programmation applicative (API) présentes sur les logiciels des appareils clients expose également au risque de capture d'empreintes numériques. Chaque logiciel, plateforme ou API va donner accès à des éléments d'information différents stockés sur l'appareil. L'API JavaScript du navigateur web, par exemple, peut fournir des informations relatives à la taille de l'écran, la profondeur des couleurs et les polices système disponibles. D'autres API demanderont l'accès à des éléments d'information stockés dans le micrologiciel (p. ex. le type de processeur), le système d'exploitation (p.ex. le type de SE) ou le modèle de carte graphique[22]. Les requêtes API peuvent également révéler la présence de logiciels installés (p.ex. des modules d'extension de navigateur), voire leurs numéros de version précis. L'accès à ces ensembles d'informations augmente le nombre de bits d'information (entropie) et donc le risque de reconnaissance d'une personne au moyen de son appareil[23].

À la différence des cookies HTTP, la capture d'empreintes numériques peut opérer de manière clandestine[24]. L'utilisateur ne dispose d'aucun moyen simple d'empêcher cette activité et les possibilités de réinitialiser ou de modifier les éléments d'information utilisés pour générer l'empreinte numérique sont rares. En conséquence, des tiers sont en mesure d'exploiter les empreintes numériques pour identifier ou individualiser des utilisateurs à leur insu, en vue de cibler des contenus ou de soumettre d'une manière ou d'une autre les personnes concernées à un traitement différencié.

Dans son avis 16/2011[25], le GT29 note que les entreprises publicitaires font valoir que l'utilisation de codes ou d'autres valeurs uniques n'implique pas le traitement de données à caractère personnel. Cette argumentation est en contradiction avec la finalité d'un traitement destiné à la présentation de contenus et de publicités personnalisés, qui est de communiquer directement avec une personne précise. Le GT29 a déclaré à plusieurs reprises que de tels identifiants uniques constituent des données à caractère personnel[26].

---

[22] Mowery, 2012. *Pixel Perfect: Fingerprinting Canvas in HTML5*. http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf

[23] Mozilla, 2014. https://wiki.mozilla.org/Fingerprinting

[24] Dans certains cas seulement – par exemple la spécification de l'API de géolocalisation HTML5 – le protocole exige la transmission d'un signal à l'utilisateur. Voir http://www.w3.org/TR/geolocation-API/#privacy_for_uas

[25] Groupe de travail «Article 29», 2014. Avis 16/2011 sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_fr.pdf

[26] Groupe de travail «Article 29», 2014. Avis 05/2014 sur les techniques d'anonymisation, p. 13. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

6. Cadre juridique

Dès lors qu'une empreinte numérique est générée par le stockage d'informations, ou l'accès à des informations stockées, dans l'équipement terminal de l'utilisateur, la directive «vie privée et communications électroniques» s'applique.

Ainsi qu'il est exposé dans l'avis 04/2012, l'article 5, paragraphe 3, permet d'exempter un traitement de l'obligation de consentement s'il satisfait à l'un des critères suivants:

CRITÈRE A: stockage ou accès techniques «visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques».

CRITÈRE B: stockage ou accès techniques «*strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur*».

En outre, l'exploitant du site web est tenu de respecter la signification définie de tous autres signaux indiquant les préférences de l'utilisateur à cet égard – tel que l'en-tête Do Not Track[27] («Pas de pistage»)[28].

Bien que l'application de la directive sur la protection des données ne relève pas du champ d'application du présent avis, dès l'instant où la capture d'empreintes numérique est constitutive d'un traitement de données à caractère personnel, elle doit impérativement respecter chacune des dispositions pertinentes de cette directive.

L'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» fait obligation à toute partie souhaitant stocker des informations, ou accéder à des informations déjà stockées, dans l'équipement terminal de l'utilisateur d'obtenir le consentement préalable de ce dernier, même si ces informations ne sont pas encore considérées comme des données à caractère personnel. Le GT29 s'est penché sur la question du consentement dans plusieurs avis, tant d'un point de vue général[29] qu'en ce qui concerne plus particulièrement la publicité comportementale en ligne[30]. Le groupe de travail a

[27] W3C, 2015. *Tracking Preference Expression (DNT)*. http://www.w3.org/TR/tracking-dnt/

[28] Le protocole « Do Not Track» pourrait servir, dans certaines circonstances, de mécanisme de gestion du consentement au niveau le plus fin possible, dans le respect du considérant 66 de la directive 2009/136/CE. Ce considérant permet aux utilisateurs d'exprimer leur consentement par le biais des paramètres de leur navigateur, mais seulement si ce consentement satisfait aux conditions de validité précitées. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

[29] Groupe de travail «Article 29», 2011. Avis 15/2011 sur la définition du consentement. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf

[30] Groupe de travail «Article 29», 2010. Avis 2/2010 sur la publicité comportementale en ligne. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp171_fr.pdf

également examiné l'obligation de consentement dans le contexte de l'article 5, paragraphe 3, et des cookies[31].

Il y a lieu de rappeler que, dans son avis 02/2013 sur les applications destinées aux dispositifs intelligents[32], le GT29 observait:

«*[L]e consentement requis pour placer ou lire une quelconque information dans un dispositif se distingue du consentement nécessaire à l'obtention d'une base juridique autorisant le traitement de différents types de données à caractère personnel. Bien que ces deux obligations de consentement soient simultanément applicables, […] les deux types de consentement peuvent être fusionnés dans la pratique […], pour autant que l'utilisateur ait pris conscience, sans aucune ambiguïté, de l'autorisation qu'il s'apprête à accorder.*»

Le considérant 66 de la directive 2009/136/CE fait référence à une «*intrusion non autorisée dans la sphère privée*», et l'article 5 de la directive «vie privée et communications électroniques» a pour objet l'obligation de confidentialité des communications. L'article 5, paragraphe 3, peut être considéré comme étendant la confidentialité des informations à celles qui sont stockées ou accessibles dans l'appareil de l'utilisateur. Dès lors, tout traitement entrepris par un tiers, qui agit sur le comportement de cet appareil ou qui, d'une manière ou d'une autre, lui fait stocker des informations, y donner accès en lui-même ou les exposer par son moyen entre dans le champ d'application de l'article 5, paragraphe 3.

L'utilisation des termes «*stockées ou accessibles*» indique qu'il n'est pas obligatoire que le stockage et l'accès interviennent au cours de la même communication, pas plus qu'il n'est nécessaire qu'ils soient effectués par la même partie. Les informations stockées par une partie (y compris celles stockées par l'utilisateur ou le fabricant de l'appareil) auxquelles accède ultérieurement une autre partie relèvent donc du champ de l'article 5, paragraphe 3. Considérons l'exemple d'une appli de téléphone portable qui traite la liste des contacts de l'utilisateur, lorsque les coordonnées sont stockées par l'utilisateur lui-même, mais que l'accès est effectué par le tiers. Il serait erroné d'interpréter cela comme signifiant que le tiers n'a pas besoin de consentement pour accéder à ces informations du simple fait que ce n'est pas lui qui les a stockées. L'obligation de consentement s'applique également lors de l'accès à une valeur en lecture seule (p. ex. lors du recueil de l'adresse MAC d'une interface réseau via l'API du système d'exploitation).

Il est donc important que les tiers se souviennent qu'à partir du moment où la capture d'empreintes numériques requiert le stockage (d'un ensemble) d'informations, ou l'accès à des informations (ou à un ensemble d'informations) dans l'appareil de l'utilisateur, le consentement préalable de ce dernier est obligatoire (à moins qu'une exemption valable ne s'applique). Cela reste vrai même si certains de ces éléments d'information n'ont pas nécessité le stockage d'informations ou l'accès à des informations.

---

[31] Groupe de travail «Article 29», 2013. Document de travail n° 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_fr.pdf

[32] Groupe de travail «Article 29», 2013. Avis 02/2013 sur les applications destinées aux dispositifs intelligents. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf

7. Scénarios d'utilisation des empreintes numériques

7.1. Étude de cas: analytique de site web d'origine

Plusieurs services en ligne ont proposé la capture d'empreintes numériques comme une solution de rechange aux cookies HTTP à des fins analytiques permettant de faire l'économie du consentement prévu à l'article 5, paragraphe 3. Dans son avis 04/2012, le groupe de travail a reconnu la nécessité d'une troisième exemption de l'obligation de consentement en faveur de l'analytique d'origine:

«*lorsqu[e les cookies d'analyse d'origine] sont strictement limités à l'établissement de statistiques agrégées concernant l'origine et lorsqu'ils sont utilisés par des sites web qui fournissent déjà des informations claires sur ces cookies dans leurs dispositions relatives à la protection de la vie privée, ainsi que des garanties adéquates en la matière. Ces garanties devraient comprendre un dispositif facile à utiliser permettant de ne pas participer aux mécanismes de collecte de données et d'anonymisation intégrale qui sont appliqués à d'autres informations identifiables collectées telles que les adresses IP*.»

Toutefois, il indiquait également, dans le même avis, qu'il n'existait pas, à l'heure actuelle, d'exemption de l'obligation de consentement pour les cookies strictement limités à l'établissement de statistiques anonymisées et agrégées concernant le domaine d'origine[33]. Par conséquent, l'analytique mise en place par le site web d'origine au moyen de la capture d'empreintes numériques ne relève pas de l'exemption définie par le CRITÈRE A ou B, et le consentement de l'utilisateur est requis.

7.2. Étude de cas: pistage à des fins de publicité comportementale en ligne

De nombreux sites web comportent des pixels espions, des balises invisibles ou des codes JavaScript pour l'activation de services publicitaires. Cela se traduit par l'émission de requêtes visant à collecter des éléments d'information dans l'appareil de l'utilisateur. Ces requêtes sont transmises aux tiers prestataires de services publicitaires et leur permettent de générer une empreinte numérique avec laquelle ils pisteront l'utilisateur dans la durée et d'un site web à l'autre, comme de créer un profil d'intérêts pour l'envoi de publicités ciblées, même si l'utilisateur refuse les cookies. Techniquement, ce traitement peut se faire de manière clandestine, à l'insu de l'utilisateur.

Dans son avis 04/2012, le GT29 souligne que les publicités de tiers ne relèvent pas de l'exemption définie par le CRITÈRE A ou B. La capture d'empreintes numériques à des fins de publicité ciblée exige donc le consentement de l'utilisateur.

7.3. Étude de cas: fourniture de réseau

La bonne gestion d'un réseau implique le transfert de certains éléments d'information liés à chaque appareil connecté au réseau. Par exemple, un point d'accès Wi-Fi qui gère la connexion entre des dispositifs sans fil et un réseau filaire traitera des éléments d'information univoques et non univoques

[33] Groupe de travail «Article 29», 2012. Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies, p. 11-12.

tels que l'adresse MAC[34] et le canal, afin de gérer correctement les connexions et d'acheminer correctement les paquets de données.

Dès lors que la fourniture du réseau suppose des éléments d'information qui stockent des informations, ou obtiennent l'accès à des informations, dans l'appareil de l'utilisateur, un tel traitement entre dans le champ d'application de l'article 5, paragraphe 3. S'il est nécessaire au fonctionnement normal du réseau, ce traitement sera exempté au titre du CRITÈRE A.

L'utilisation secondaire d'un élément d'information ou d'une empreinte numérique à des fins de pistage n'est pas considérée comme «*visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques*» ou «*strictement nécessair[e] au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur*». Lors de l'examen des cookies polyvalents dans son avis 04/2012, le GT29 observe qu'«*il est très peu probable que le pistage soit conforme au CRITÈRE A ou B*», de sorte que, si un tiers souhaite exploiter une empreinte numérique à des fins multiples, il ne sera «*exempté de l'obligation de consentement que si l'ensemble des différentes finalités […] sont individuellement exemptées de cette obligation*».

7.4. Étude de cas: contrôle d'accès utilisateur

Un service en ligne pourrait vouloir utiliser la capture d'empreinte numérique pour renforcer son contrôle d'accès utilisateur (c'est-à-dire en combinaison avec un nom d'utilisateur et un mot de passe). Il est possible de recourir à l'empreinte numérique pour s'assurer qu'un compte est lié à un appareil en particulier, de telle manière que cet appareil serve de deuxième facteur d'identification.

Par exemple, un service d'abonnement musical ne permet à l'utilisateur d'accéder à son service qu'à partir d'un nombre restreint d'appareils déterminés. Si l'utilisateur a déjà utilisé cet appareil, l'exploitant du site web peut décider d'exécuter moins de contrôles avant de lui accorder l'accès.

Dès lors qu'une empreinte numérique est composée d'éléments d'information qui stockent des informations, ou obtiennent l'accès à des informations, dans l'appareil de l'utilisateur, elle entre dans le champ d'application de l'article 5, paragraphe 3. Ces finalités ne sauraient cependant être considérées comme «*strictement nécessaires*» à la fourniture d'une fonctionnalité expressément demandée par l'utilisateur; partant, le consentement valable de l'utilisateur est requis.

Les exploitants de sites web seront peut-être amenés à envisager la mise en place d'un éventail de contrôles adéquats et proportionnés, ou de toute autre méthode d'authentification (p. ex. mot de passe à utilisation unique, confirmation secondaire par courrier électronique).

7.5. Étude de cas: sécurité centrée sur l'utilisateur

Dans son avis 04/2012, le GT29 indique que les «*cookies mis en place dans le but spécifique de renforcer la sécurité du service expressément demandé par l'utilisateur*» (par exemple, pour détecter plusieurs tentatives infructueuses de connexion) sont exemptés au titre du CRITÈRE B.

[34] Normalement, l'adresse MAC identifie de manière unique chaque appareil connecté au réseau. En outre, le préfixe de l'adresse MAC désigne le fabricant de la puce.

Cette exemption est également applicable à la capture d'empreinte numérique, mais, comme pour les cookies, elle «*ne couvrirait […] pas l'utilisation [d'empreintes] se rapportant à la sécurité des sites web ou aux services de tiers qui n'ont pas été expressément demandés par l'utilisateur*».

Des données collectées au moyen d'une empreinte numérique pour répondre à une finalité de sécurité centrée sur l'utilisateur ne peuvent bénéficier de l'exemption du consentement qu'à la condition de ne pas être utilisées pour une finalité secondaire, quelle qu'elle soit. Des garanties techniques et organisationnelles doivent être mises en place pour empêcher toute utilisation secondaire des données d'empreinte numérique, généralement conservées dans les fichiers journaux de sécurité du serveur.

7.6. Étude de cas: adaptation de l'interface utilisateur à l'appareil

Il peut être utile d'avoir accès à des informations relatives à l'appareil, comme la taille de l'écran, pour optimiser la présentation du contenu[35]. Par exemple, un site de média en ligne passera en mode «basse résolution» ou à la présentation sur une seule colonne pour les appareils mobiles. Ou encore, un site web – ou les tiers servant des contenus par l'intermédiaire de ce site – interrogera l'appareil pour déterminer ses capacités techniques, par exemple les formats vidéo pris en charge.

Lorsqu'un tiers demande l'accès à des informations stockées dans l'appareil de l'utilisateur à la seule fin d'adapter le contenu aux caractéristiques de cet appareil, le CRITÈRE B est satisfait. Le consentement de l'utilisateur n'est donc pas requis pour une personnalisation ponctuelle de l'interface utilisateur.

Si toutefois ces informations sont également exploitées pour des finalités secondaires, l'exemption ne s'applique plus.

8. Conclusions

Le présent avis se penche sur la question de la capture d'empreintes numériques et sur l'applicabilité de l'article 5, paragraphe 3, de la directive 2002/58/CE «vie privée et communications électroniques», modifiée par la directive 2009/136/CE, sans préjudice des dispositions de la directive 95/46/CE sur la protection des données. Il complète l'avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies et confirme que, dans un certain nombre de cas, cette technologie passe par le stockage d'informations, ou l'obtention de l'accès à des informations, dans l'appareil de l'utilisateur. L'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique donc également à la capture d'empreintes numériques sous diverses formes.

En conséquence, les parties qui souhaitent traiter des empreintes numériques générées par l'obtention de l'accès à des informations ou le stockage d'informations dans l'équipement terminal de l'utilisateur doivent obtenir au préalable le consentement valable de ce dernier (à moins qu'une exemption ne s'applique).

[35] Il convient de noter que l'on peut atteindre cet objectif en recourant à des méthodes moins intrusives pour la vie privée, par exemple en utilisant la chaîne «agent utilisateur».