Lignes directrices 2/2023 sur le champ d'application technique de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques

Version 2.0

Adoptées le 7 octobre 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Historique de la version

Version 1.0	14 novembre 2023	Adoption des lignes directrices pour consultation publique
Version 2.0	7 octobre 2024	Adoption des lignes directrices après consultation publique

Synthèse

Dans les présentes lignes directrices, le comité européen de la protection des données (ci-après le «comité») examine l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques à différentes solutions techniques. Les présentes lignes directrices s'appuient sur l'avis 9/2014 du groupe de travail «article 29» sur l'application de la directive vie privée et communications électroniques à la capture d'empreintes numériques et visent à fournir une compréhension claire des opérations techniques couvertes par l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

L'apparition de nouvelles méthodes de pistage destinées à remplacer les outils de pistage existants (par exemple, les cookies, en raison de l'arrêt de la prise en charge des cookies tiers par certains fournisseurs de navigateurs) et à créer de nouveaux modèles commerciaux est devenue une préoccupation majeure en matière de protection des données. Bien que l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques soit solidement établie et que cette disposition soit mise en œuvre à l'égard de certaines technologies de pistage, telles que les cookies, il est nécessaire de lever les ambiguïtés liées à l'application de ladite disposition aux outils de pistage émergents.

Les lignes directrices recensent trois éléments clés aux fins de l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques (section 2.1), à savoir les «informations», l'«équipement terminal d'un abonné ou d'un utilisateur» et l'«obtention de l'accès», ainsi que le «stockage d'informations et les informations stockées». Les lignes directrices fournissent en outre une analyse détaillée de chaque élément (sections 2.2 à 2.6).

Dans la section 3, cette analyse est appliquée à une liste non exhaustive de cas d'utilisation correspondant à des techniques communes, à savoir:

- le pistage au moyen d'URL et de pixel
- le traitement local
- le pistage fondé uniquement sur l'IP
- la communication intermittente et intermédiée relative à l'internet des objets (IoT)
- l'identificateur unique

Table des matières

Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point e), du 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 (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du comité mixte de l'EEE nº 154/2018 du 6 juillet 2018 ([1]),

vu l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil 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, telle que modifiée par la directive 2009/136/CE (ci-après la directive vie privée et communications électroniques),

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1 INTRODUCTION

1. Conformément à l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, «*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 autorisé que sur le fondement d'un accord ou d'une nécessité résultant des finalités spécifiques énoncées dans cette disposition. Ainsi qu'il est rappelé au considérant 24 de la directive vie privée et communications électroniques ([2]), l'objectif de cette disposition est de protéger les équipements terminaux des utilisateurs, étant donné qu'ils relèvent de leur vie privée. Il ressort du libellé de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques que celui-ci ne s'applique pas exclusivement aux cookies, mais également aux «technologies similaires». Toutefois, il n'existe actuellement aucune liste exhaustive des opérations techniques couvertes par l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

2. Il était déjà précisé dans l'avis 9/2014 du groupe de travail «article 29» sur l'application de la directive vie privée et communications électroniques à la capture d'empreintes numériques (ci-après l'«avis 9/2014 du groupe de travail "article 29"») que la capture d'empreintes numériques relève du champ d'application technique de l'article 5, paragraphe 3, de la directive vie privée et

([1]) Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
([2]) «L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Or, les logiciels espions, les pixels invisibles (web bugs), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée de ce dernier. L'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné».

communications électroniques ([3]), mais qu'en raison des nouvelles avancées technologiques, des orientations supplémentaires sont nécessaires en ce qui concerne les techniques de pistage actuellement observées. Le paysage technique a évolué au cours de la dernière décennie, avec l'utilisation croissante d'identificateurs intégrés dans les systèmes d'exploitation, ainsi que la création de nouveaux outils permettant le stockage d'informations dans les équipements terminaux.

3. Les ambiguïtés relatives au champ d'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques ont incité à la mise en œuvre de solutions de substitution aux fins du pistage des utilisateurs de l'internet et ont conduit à une tendance à contourner les obligations légales prévues par cette disposition. Toutes ces situations soulèvent des préoccupations et rendent nécessaire une analyse supplémentaire afin de compléter les précédentes orientations du comité.

4. L'objectif des présentes lignes directrices est la conduite d'une analyse technique du champ d'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, à savoir la clarification de ce qui est techniquement couvert par l'expression «*de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur*». Les présentes lignes directrices ne traitent pas des circonstances dans lesquelles une opération de traitement peut relever des exemptions à l'obligation de recueillir l'accord prévues par la directive vie privée et communications électroniques ([4]), étant donné que ces circonstances devraient être analysées au cas par cas, en tenant compte de la ou des transpositions pertinentes par les États membres et des orientations publiées par les autorités nationales compétentes.

5. Une liste non exhaustive de cas d'utilisation spécifiques sera analysée dans la dernière partie des présentes lignes directrices.

2 ANALYSE

2.1 Éléments clés aux fins de l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques

6. L'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique si:

   a. **CRITÈRE A:** les opérations effectuées concernent des «informations». Il convient de noter que le terme utilisé n'est pas «données à caractère personnel», mais «informations».

   b. **CRITÈRE B:** les opérations effectuées concernent un «*équipement terminal*» d'un abonné ou d'un utilisateur (B.1), ce qui implique la nécessité d'évaluer la notion de «*réseau public de communications*» (B.2).

   c. **CRITÈRE C:** les opérations effectuées constituent effectivement un «*stockage*» (C.1) ou une «*obtention de l'accès*» (C.2). Ces deux notions peuvent être étudiées indépendamment, comme le rappelle l'avis 9/2014 du groupe de travail «Article 29»: *«[l]'utilisation des termes "stockées ou accessibles" indique qu'il n'est pas obligatoire que le stockage et l'accès interviennent au cours de*

([3]) Avis 9/2014 du groupe de travail «Article 29», page 12.
([4]) Comme l'indique l'article 5, paragraphe 3, de la directive vie privée et communications électroniques: «*[c]ette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur*.»

la même communication, pas plus qu'il n'est nécessaire qu'ils soient effectués par la même partie» ([5]).

Par souci de lisibilité, l'entité qui obtient l'accès aux informations stockées dans l'équipement terminal de l'utilisateur sera ci-après dénommée l'«entité accédante».

2.2 Notion d'«informations» – Critère A

7. Comme indiqué dans le CRITÈRE A, cette section détaille ce que recouvre la notion d'«informations». Le choix du terme «informations», qui recouvre une catégorie plus large que la simple notion de données à caractère personnel, est lié au champ d'application de la directive vie privée et communications électroniques.

8. L'objectif de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques est de protéger la vie privée des utilisateurs, comme l'indique son considérant 24: «*[l]'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*.» Celle-ci est également protégée par l'article 7 de la charte des droits fondamentaux de l'Union européenne.

9. En fait, les scénarios qui entraînent un empiétement sur cette vie privée, même s'ils ne concernent pas de données à caractère personnel, sont explicitement couverts par le libellé de l'article 5, paragraphe 3, et du considérant 24 de la directive vie privée et communications électroniques, par exemple le stockage de virus sur l'équipement terminal de l'utilisateur. Cela montre que la définition du terme «informations» ne saurait se limiter à la propriété d'être liée à une personne physique identifiée ou identifiable.

10. Ce point a été confirmé par la Cour de justice de l'UE: «*[c]ette protection s'applique à toute information stockée sur cet équipement terminal, indépendamment du fait qu'il s'agisse ou non de données à caractère personnel et vise, notamment, comme il ressort de ce même considérant, à protéger les utilisateurs contre le risque que des identificateurs cachés ou autres dispositifs analogues pénètrent dans l'équipement terminal de ces utilisateurs à leur insu*» ([6]).

11. La question de savoir si l'origine de ces informations et les raisons pour lesquelles elles sont stockées dans l'équipement terminal doivent être prises en considération lors de l'évaluation de l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques a été clarifiée précédemment. Par exemple, l'avis 9/2014 du groupe de travail «Article 29» explique ce qui suit: «*[i]l 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)*» ([7]).

12. En conclusion, la notion d'«informations» comprend à la fois des données à caractère non personnel et des données à caractère personnel, indépendamment de la manière dont ces données ont été stockées et par qui, c'est-à-dire par une entité externe (y compris également d'autres entités que celle qui possède l'accès), par l'utilisateur, par un fabricant ou dans tout autre scénario.

([5]) Avis 9/2014 du groupe de travail «Article 29», page 9.
([6]) Arrêt de la Cour de justice du 1er octobre 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, point 70.
([7]) Avis 9/2014 du groupe de travail «Article 29», page 9.

2.3 Notion d'«équipement terminal d'un abonné ou d'un utilisateur» – Critère B.1

13. Cette section s'appuie sur la définition utilisée dans la directive 2008/63/CE, telle que référencée à l'article 2 de la directive (UE) 2018/1972; l'«équipement terminal» y est défini comme suit: «*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*» ([8]).

14. Le considérant 24 de la directive vie privée et communications électroniques permet une compréhension claire du rôle de l'équipement terminal dans la protection offerte par l'article 5, paragraphe 3, de ladite directive. La directive vie privée et communications électroniques protège la vie privée des utilisateurs non seulement en ce qui concerne la confidentialité de leurs informations, mais aussi en préservant l'intégrité de leurs équipements terminaux. L'interprétation de la notion d'équipement terminal sera fondée sur cette compréhension tout au long des présentes lignes directrices.

15. L'article 3 de la directive vie privée et communications électroniques dispose que, pour que la directive puisse s'appliquer, le traitement des données à caractère personnel doit être effectué dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications. Cela implique qu'un dispositif devrait être utilisable en rapport avec un tel service et que, pour être qualifié de terminal, un équipement devrait être connecté ou connectable ([9]) à l'interface d'un réseau public de communications. Le comité note que les modifications apportées en 2009 ([10]) au texte de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques ont étendu la protection des équipements terminaux en supprimant la référence à l'«utilisation des réseaux de communications électroniques» en tant que moyen de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal. Par conséquent, tant qu'un dispositif possède une interface réseau qui le rend compatible avec une connexion (même si une telle connexion n'est pas en place), l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique à toute entité qui stockerait des informations et accéderait à des informations déjà stockées dans l'équipement terminal, quels que soient les moyens d'accès à l'équipement terminal et qu'il soit connecté ou non à un réseau.

([8]) Directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux de télécommunications (version codifiée), article 1er, paragraphe 1.
([9]) En d'autres termes, il dispose des capacités techniques pour être connecté au réseau, même si cette connexion n'est pas actuellement en place.
([10]) Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs (Texte présentant de l'intérêt pour l'EEE), JO L 337 du 18.12.2009, article 2, paragraphe 5 et considérant 65.

16. Les équipements qui font partie du réseau public de communications électroniques lui-même ne seraient pas considérés comme des équipements terminaux au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électronique ([11]).

17. Un équipement terminal peut être constitué d'un nombre quelconque d'éléments matériels individuels qui, ensemble, constituent l'équipement terminal. Il peut s'agir ou non d'un dispositif physiquement fermé, qui héberge l'ensemble du matériel d'affichage, de traitement et de stockage, ainsi que les périphériques (par exemple, téléphones intelligents, ordinateurs portables, dispositifs de stockage connectés au réseau, voitures connectées ou téléviseurs connectés, lunettes intelligentes).

18. La directive vie privée et communications électroniques reconnaît que la protection de la confidentialité des informations stockées sur l'équipement terminal d'un utilisateur et l'intégrité de l'équipement terminal dudit utilisateur ne se résument pas à la protection de la vie privée des personnes physiques, mais touchent aussi au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales ([12]). Dès lors, un équipement terminal qui rend possible cette correspondance et la réalisation des intérêts légitimes des personnes morales est protégé en vertu de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

19. L'utilisateur ou l'abonné peut être propriétaire de l'équipement terminal, le louer ou le recevoir de toute autre manière. Plusieurs utilisateurs ou abonnés peuvent partager le même équipement terminal.

20. Cette protection garantie par la directive vie privée et communications électroniques s'applique à l'équipement terminal associé à l'utilisateur ou à l'abonné, et ne dépend pas du fait que l'utilisateur ait ou non mis en place les moyens d'accès (par exemple s'il a lancé la communication électronique) ni même du fait que l'utilisateur ait ou non connaissance desdits moyens d'accès.

2.4 Notion de «réseau public de communications» – Critère B.2

21. Étant donné que la situation régie par la directive vie privée et communications électroniques est celle liée à «*la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté*» ([13]) et que la définition d'un équipement terminal mentionne spécifiquement la notion de «*réseau public de communications*», il est essentiel de clarifier cette notion afin de déterminer le contexte dans lequel l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique.

22. La notion de réseau de communications électroniques n'est pas définie dans la directive vie privée et communications électroniques elle-même. Cette notion a été mentionnée pour la première fois dans la directive 2002/21/CE (directive «cadre») relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques ([14]), remplacée ensuite par l'article 2, paragraphe 1, de la directive 2018/1972 (le code des communications électroniques européen). Elle est désormais définie comme suit:

([11]) Pour identifier les limites s'appliquant au terme «réseau» dans différents contextes, reportez-vous aux lignes directrices de l'ORECE sur des approches communes pour l'identification du point de terminaison du réseau dans différentes topologies de réseau [BoR (20) 46].
([12]) En effet, comme le rappelle l'article 2, paragraphe 13, de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen, l'utilisateur peut être une personne physique ou morale.
([13]) Article 3 de la directive vie privée et communications électroniques.
([14]) Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre»).

On entend par «réseau de communications électroniques», les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise ([15]).

23. Cette définition est neutre en ce qui concerne les technologies de transmission: un réseau de communications électroniques désigne tout système réseau permettant la transmission de signaux électroniques entre ses nœuds, indépendamment de l'équipement et des protocoles utilisés.

24. La notion de réseau de communications électroniques au sens de la directive (UE) 2018/1972 ne dépend pas de la nature publique ou privée de l'infrastructure, ni de la manière dont le réseau est déployé ou géré [«*qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée*» ([16])]. En conséquence, la définition du réseau de communications électroniques, au sens de l'article 2 de la directive (UE) 2018/1972, est suffisamment large pour couvrir n'importe quel type d'infrastructure. Elle inclut les réseaux gérés ou non par un opérateur, les réseaux cogérés par un groupe d'opérateurs, voire les réseaux ad hoc, au sein desquels un équipement terminal peut rejoindre ou quitter dynamiquement un maillage composé d'autres équipements terminaux à l'aide de protocoles de transmission à courte portée.

25. Cette définition du réseau ne prévoit aucune limite en ce qui concerne le nombre d'équipements terminaux présents dans le réseau à tout moment. Certains systèmes de mise en réseau reposent sur des nœuds relayant des informations de manière ad hoc vers des nœuds actuellement connectés ([17]) et sont susceptibles, à un moment donné, de n'avoir que deux pairs qui communiquent. Ces cas relèveraient du champ d'application général de la directive vie privée et communications électroniques, pour autant que le protocole du réseau permette d'inclure d'autres pairs.

26. La disponibilité publique du réseau de communications est nécessaire pour que le dispositif soit considéré comme un équipement terminal et, partant, pour l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques. Il convient de noter que le fait que le réseau soit mis à la disposition d'un sous-ensemble limité du public (par exemple, des abonnés, payants ou non, auxquels s'appliquent des conditions d'éligibilité) n'a pas pour conséquence qu'un tel réseau est privé ([18]).

([15]) Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte) (Texte présentant de l'intérêt pour l'EEE), article 2, paragraphe 1.

([16]) Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte) (Texte présentant de l'intérêt pour l'EEE), article 2, paragraphe 1.

([17]) Par exemple, dans le contexte d'un système de mise en réseau tolérant aux délais qui met en œuvre des «techniques de stockage et de transfert», tel que le projet Briar open source.

([18]) Pour une analyse plus approfondie de l'identification des réseaux publics de communications, veuillez vous référer aux lignes directrices de l'ORECE pour la mise en œuvre du règlement relatif à l'accès à un internet ouvert [BoR (20) 112].

2.5 Notion d'«obtention de l'accès» – critère C.1

27. Afin de définir correctement la notion d'«obtention de l'accès», il est important de tenir compte du champ d'application de la directive vie privée et communications électroniques, énoncé à son article 1er: «*assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté*».

28. En résumé, la directive vie privée et communications électroniques est un instrument juridique qui préserve la vie privée et vise à protéger la confidentialité des communications et l'intégrité des dispositifs. Au considérant 24 de la directive vie privée et communications électroniques, il est précisé que, dans le cas d'une personne physique, l'équipement terminal de l'utilisateur relève de sa vie privée et que l'accès aux informations qui y sont stockées à son insu peut porter gravement atteinte à sa vie privée.

29. Les personnes morales sont également protégées par la directive vie privée et communications électroniques ([19]). Par conséquent, la notion d'«obtention de l'accès» au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques doit être interprétée d'une manière qui préserve ces droits contre toute violation par des tiers.

30. Le stockage des informations et l'obtention de l'accès peuvent être des opérations distinctes, effectuées par des entités indépendantes. Il n'est pas nécessaire que le stockage des informations et l'accès aux informations déjà stockées existent tous deux pour que l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique.

31. Comme l'indique l'avis 9/2014 du groupe de travail «Article 29»: «*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*» ([20]). Par conséquent, aucune restriction n'est imposée quant à l'origine des informations sur l'équipement terminal aux fins de l'application de la notion d'«accès».

32. Chaque fois qu'une entité prend des mesures en vue d'obtenir l'accès à des informations stockées dans l'équipement terminal, l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique. En général, cela implique que l'entité accédante envoie de manière proactive des instructions spécifiques à l'équipement terminal afin de recevoir en retour les informations ciblées. C'est le cas, par exemple, des cookies, pour lesquels l'entité accédante demande à l'équipement terminal d'envoyer des informations de manière proactive lors de chaque requête HTTP (protocole de transfert hypertexte) ultérieure.

33. Tel est également le cas lorsque l'entité accédante distribue, sur l'équipement terminal de l'utilisateur, un logiciel qui est stocké et appellera ensuite de manière proactive un point terminal d'interface de programmation d'application (ci-après «API») sur le réseau. Parmi les autres exemples, on peut citer un code JavaScript, dans lequel l'entité accédante demande au navigateur de l'utilisateur d'envoyer des requêtes asynchrones contenant les informations ciblées. Un tel accès relève clairement du champ d'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques,

([19]) Considérant 26 de la directive vie privée et communications électroniques, voir point 17 ci-dessus.
([20]) Avis 9/2014 du groupe de travail «Article 29», page 9.

étant donné que l'entité accédante demande explicitement à l'équipement terminal de transmettre les informations.

34. Dans certains cas, l'entité qui demande à l'équipement terminal de renvoyer les données ciblées et l'entité qui reçoit les informations peuvent ne pas être les mêmes. Cela peut résulter de la mise à disposition et/ou de l'utilisation d'un mécanisme commun entre les deux entités. Le fait de demander au dispositif d'envoyer des informations déjà stockées [par exemple, par l'intermédiaire d'un protocole ou d'un SDK ([21]), ce qui implique la transmission proactive d'informations par l'équipement terminal] rend possible une intrusion dans l'équipement terminal, de sorte qu'un tel accès déclenche l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques. Comme indiqué dans l'avis 09/2014 du groupe de travail «Article 29», cela peut être le cas lorsqu'un site web demande à l'équipement terminal d'envoyer des informations à des services publicitaires tiers par le biais de l'inclusion d'un pixel espion ([22]). Ce cas d'utilisation est développé plus en détail à la section 3.1.

2.6 Notions de «stockage d'informations» et d'«informations stockées» - Critère C.2

35. Le stockage d'informations au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques désigne le placement d'informations sur un support de stockage électronique physique qui fait partie de l'équipement terminal d'un utilisateur ou d'un abonné ([23]).

36. En règle générale, les informations ne sont pas stockées dans l'équipement terminal d'un utilisateur ou d'un abonné par le biais d'un accès direct à la mémoire de l'appareil par une autre partie, mais plutôt en demandant au logiciel de l'équipement terminal de générer des informations spécifiques. Le stockage découlant de ces instructions est considéré comme étant effectué directement par l'autre partie. Cela inclut l'utilisation de protocoles établis tels que le stockage de cookies dans les navigateurs, ainsi que de logiciels personnalisés, quelle que soit la personne qui a créé ou installé les protocoles ou les logiciels sur l'équipement terminal.

37. La directive vie privée et communications électroniques ne fixe aucune limite supérieure ou inférieure à la durée pendant laquelle l'information doit demeurer sur un support de stockage pour être considérée comme stockée, pas plus qu'elle ne fixe de limite supérieure ou inférieure à la quantité d'informations à stocker.

38. De même, la notion de stockage ne dépend pas du type de support sur lequel les informations sont stockées. Les exemples typiques incluent les disques durs («HDD»), les disques SSD, la mémoire morte programmable effaçable électriquement («EEPROM») et la mémoire à accès aléatoire («RAM»), mais les scénarios moins courants comportant l'utilisation de supports tels qu'une bande magnétique ou la mémoire cache d'une d'unité centrale de traitement («CPU») ne sont pas exclus du champ d'application. Le support de stockage peut être connecté en interne (par exemple, au moyen d'une connexion SATA) ou en externe (par exemple, par le biais d'une connexion USB).

39. Les «informations stockées» désignent les informations déjà présentes sur l'équipement terminal, indépendamment de la source ou de la nature de ces informations. Cela inclut tout résultat du stockage d'informations au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, tel que décrit ci-dessus (soit par la même partie qui obtiendrait

([21]) Un SDK («software development kit») est un ensemble d'outils de développement logiciel permettant de faciliter la création de logiciels d'application.
([22]) Avis 9/2014 du groupe de travail «Article 29», page 10.
([23]) Tel que défini à la section 2.3 des présentes lignes directrices.

ultérieurement l'accès, soit par une autre tierce partie). Sont également inclus les résultats des processus de stockage d'informations qui ne relèvent pas de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, comme le stockage sur l'équipement terminal par l'utilisateur ou l'abonné lui-même, ou par un fabricant de matériel (comme les adresses MAC des contrôleurs d'interface réseau), les capteurs intégrés dans l'équipement terminal ou les processus et programmes exécutés sur l'équipement terminal, qui peuvent ou non produire des informations qui dépendent ou découlent des informations stockées.

3 CAS D'UTILISATION

40. Comme indiqué dans l'introduction des présentes lignes directrices ([24]), celles-ci ne contiennent pas d'analyse de l'application des exemptions à l'obligation de recueillir l'accord prévues à l'article 5, paragraphe 3, de la directive vie privée et communications électroniques. Le comité rappelle que, dans tous les cas où il y a un stockage d'informations ou l'obtention de l'accès à des informations déjà stockées, il conviendrait d'évaluer si un accord est nécessaire ou si une exemption au titre de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques peut s'appliquer. Le lecteur devrait donc examiner les exemptions dans leur cas d'utilisation, en lien avec la présente analyse technique.

41. Sans préjudice du contexte spécifique dans lequel ces catégories techniques peuvent être utilisées, qui sont nécessaires pour déterminer si l'article 5, paragraphe 3, de la directive vie privée et communications électroniques est applicable, il est possible d'identifier, de manière non exhaustive, de grandes catégories d'identificateurs et d'informations qui sont largement utilisés et qui peuvent être soumis à l'applicabilité de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

42. La communication par réseau repose généralement sur un modèle à plusieurs niveaux qui nécessite l'utilisation d'identificateurs pour permettre l'établissement et la mise en œuvre appropriés de la communication. La communication de ces identificateurs à des acteurs distants se fait par l'intermédiaire d'un logiciel qui suit des protocoles de communication convenus. Comme indiqué ci-dessus, le fait que l'entité destinataire puisse ne pas être l'entité demandant l'envoi d'informations n'empêche pas l'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques. Il peut s'agir d'identificateurs de routage tels que l'adresse MAC ou IP de l'équipement terminal, mais aussi d'identificateurs de session (SSRC, identificateur Websocket) ou de jetons d'authentification.

43. De la même manière, le protocole d'application peut inclure plusieurs mécanismes pour fournir des données contextuelles (comme l'en-tête HTTP comprenant le champ «accept» ou l'agent utilisateur), un mécanisme de mise en cache [comme ETag([25])] ou d'autres fonctionnalités [comme les cookies ou HSTS([26])]. Une fois encore, le recours à ces mécanismes pour collecter des informations [par exemple dans le cadre de la capture d'empreintes numériques([27]) ou du pistage des identificateurs de

([24]) Voir point 4 ci-dessus.
([25]) Le HTTP ETag est un identificateur qui permet de faire une requête conditionnelle sur la base de la validité des données du client mises en cache.
([26]) HTTP Strict Transport Security (HSTS) permet aux serveurs de spécifier les ressources qui doivent toujours faire l'objet de requêtes effectuées au moyen de connexions HTTPS.
([27]) Comme indiqué dans l'introduction, voir l'avis 9/2014 du groupe de travail «article 29» sur l'application de la directive vie privée et communications électroniques à la capture d'empreintes numériques.

ressources] peut conduire à l'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

44. Par ailleurs, dans certains contextes, les applications locales installées dans l'équipement terminal utilisent des informations situées strictement à l'intérieur du terminal, comme cela peut être le cas pour les API des systèmes de smartphones (accès à l'appareil photo, microphone, capteur GPS, puce accélératrice, puce radio, accès aux fichiers locaux, liste de contacts, accès aux identificateurs, etc.). Cela peut également être le cas pour les navigateurs web qui traitent des informations stockées ou générées à l'intérieur du dispositif (comme les cookies, le stockage local, WebSQL, ou même les informations fournies par les utilisateurs eux-mêmes). L'utilisation de ces informations par une application ne constituerait pas une «obtention de l'accès à des informations déjà stockées» au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, tant que les informations ne quittent pas le dispositif. Toutefois, en cas d'accès à ces informations ou à toute autre information dérivée de celles-ci, l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'appliquerait.

45. Enfin, dans certains cas, des acteurs diffusent des éléments logiciels malveillants, par exemple des logiciels de cryptominage ou, plus généralement, des maliciels, qui exploitent les capacités de traitement des équipements terminaux au profit de l'acteur distributeur. La distribution de ces logiciels malveillants dans l'équipement terminal de l'utilisateur constituerait un «stockage» au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques. En outre, si le logiciel établit une connexion réseau pour envoyer des informations à un stade ultérieur, il s'agirait d'une «obtention de l'accès» au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

46. Pour un sous-ensemble de ces catégories présentant un intérêt spécifique, soit en raison de leur usage répandu, soit parce que des explications détaillées sont justifiées au regard des circonstances de leur utilisation, une analyse connexe est fournie ci-après.

3.1 Pistage au moyen d'URL et de pixel

47. Un pixel espion est un hyperlien vers une ressource, généralement un fichier image, intégré dans un élément de contenu tel qu'un site web ou un courrier électronique. Ce pixel ne remplit généralement aucune fonction liée au contenu demandé lui-même; son seul objectif est d'établir automatiquement une communication du client à l'hôte du pixel, qui n'aurait autrement pas lieu. Ce n'est toutefois pas systématique et les pixels espions peuvent également être créés en ajoutant des informations supplémentaires aux hyperliens, ce qui permet le chargement d'images pertinentes pour le contenu présenté à l'utilisateur. L'établissement de la communication transmet diverses informations à l'hôte du pixel, en fonction du cas d'utilisation spécifique.

48. Dans le cas d'un courrier électronique, l'expéditeur peut inclure un pixel espion afin de détecter quand le récepteur lit le courrier électronique. Les pixels espions placés sur des sites web peuvent renvoyer à une entité qui recueille de nombreuses requêtes de ce type et qui est ainsi en mesure de suivre le comportement des utilisateurs. Ces pixels espions peuvent également contenir des identificateurs, métadonnées ou contenus supplémentaires dans le lien. Ces points de données peuvent être ajoutés par le propriétaire du site web, éventuellement en lien avec l'activité de l'utilisateur sur ce site, afin que des rapports analytiques d'utilisation puissent être générés. Ceux-ci peuvent également être générés de manière dynamique au moyen d'une logique applicative côté client fournie par l'entité.

49. Les liens espions peuvent fonctionner de la même manière, mais l'identificateur est ajouté à l'adresse du site web. Lorsque l'utilisateur se rend sur le localisateur uniforme de ressources (*uniform resource*

locator, «URL»), le site web ciblé charge la ressource demandée, mais collecte également un identificateur qui n'est pas pertinent sur le plan de l'identification de la ressource. Ces liens sont très couramment utilisés par les sites de commerce électronique afin d'identifier l'origine de leur source de trafic entrant. Par exemple, ces sites web peuvent fournir des liens espions à leurs partenaires. Placés sur les domaines de ces derniers, ces liens permettent aux gérants du site web de commerce électronique de déterminer lequel de ses partenaires est à l'origine d'une vente et de lui payer une commission, une pratique connue sous le nom de marketing d'affiliation.

50. Les liens et les pixels espions peuvent être distribués par un large éventail de canaux, par exemple par l'intermédiaire de courriers électroniques, de sites web, voire, dans le cas des liens espions, au moyen de n'importe quel type de système de messagerie textuelle. Cette distribution à l'équipement terminal de l'utilisateur constitue bien un stockage, à tout le moins par l'intermédiaire du mécanisme de mise en cache du logiciel côté client. De ce fait, l'article 5, paragraphe 3, de la directive vie privée et communications électroniques est applicable, même si ce stockage n'est pas permanent.

51. L'ajout d'informations de pistage aux URL ou images (pixels) envoyés à l'utilisateur constitue une demande à l'équipement terminal de renvoyer les informations ciblées (l'identificateur spécifié). Dans le cas des pixels espions développés de manière dynamique, c'est la distribution de la logique applicative (généralement un code JavaScript) qui constitue la demande. Par conséquent, il peut être considéré que le recueil d'identificateurs fournis au moyen de ces mécanismes de pistage constitue une «obtention de l'accès» au sens de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, laquelle disposition s'applique donc également à cette étape.

3.2 Traitement local

52. Certaines technologies s'appuient sur un traitement local lancé par des logiciels distribués sur les équipements terminaux des utilisateurs, les informations produites par le traitement local étant ensuite mises à la disposition d'acteurs sélectionnés par l'intermédiaire d'API côté client. Tel peut être le cas, par exemple, d'une API fournie par l'intermédiaire du navigateur web, grâce à laquelle des résultats générés localement peuvent être consultés à distance.

53. Si, à un moment donné et, par exemple, dans le code côté client, les informations traitées sont mises à la disposition d'un tiers, notamment si elles sont renvoyées à un serveur par l'intermédiaire du réseau, une telle opération (demandée par l'entité ayant élaboré le code côté client distribué sur l'équipement terminal de l'utilisateur) constituerait une «obtention de l'accès à des informations déjà stockées». Le fait que ces informations soient produites localement n'exclut pas l'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

3.3 Pistage fondé uniquement sur l'IP

54. Certains fournisseurs développent des solutions qui ne reposent que sur la collecte d'un élément, à savoir l'adresse IP, afin de surveiller la navigation ([28]) de l'utilisateur, dans certains cas au sein de plusieurs domaines. Dans ce contexte, l'article 5, paragraphe 3, de la directive vie privée et communications électroniques pourrait s'appliquer même si l'instruction de mettre à disposition l'IP a été donnée par une entité différente de celle qui l'a reçue.

([28]) Une telle opération doit être considérée en sus et indépendamment de l'utilisation et de la fonction d'une adresse IP aux fins de l'établissement et de l'acheminement ou de la transmission des communications techniques sous-jacentes, ou du fait qu'il peut s'agir ou non de données à caractère personnel (dans le cadre d'une analyse effectuée conformément à la directive vie privée et communications électroniques, il s'agit d'«informations»).

55. Toutefois, l'obtention de l'accès à des adresses IP ne déclencherait l'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques que dans les cas où ces informations proviennent de l'équipement terminal d'un abonné ou d'un utilisateur. Bien que ce ne soit pas systématiquement le cas [par exemple lorsque le NAT de classe transporteur ([29]) est activé], les adresses IPv4 sortantes statiques provenant du routeur d'un utilisateur relèveraient de ce cas, de même que les adresses IPV6, puisqu'elles sont en partie définies par l'hôte. À moins que l'entité soit en mesure de garantir que l'adresse IP ne provient pas de l'équipement terminal d'un utilisateur ou d'un abonné, elle doit prendre toutes les mesures prévues à l'article 5, paragraphe 3, de la directive vie privée et communications électroniques.

56. Bien que les présentes lignes directrices ne contiennent pas d'analyse de l'application des exemptions à l'obligation de recueillir l'accord prévues par l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, il est important de rappeler une fois de plus que l'applicabilité de cet article ne signifie pas systématiquement que l'accord doit être recueilli. Le comité rappelle donc que, dans chaque cas, il conviendrait d'évaluer si un accord est nécessaire ou si une exemption au titre de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques peut s'appliquer ([30]).

3.4 Communication intermittente et intermédiée relative à l'internet des objets

57. Les dispositifs IDO (internet des objets) produisent des informations en continu au fil du temps, par exemple grâce à des capteurs intégrés dans le dispositif, lesquelles peuvent ou non être prétraitées localement. Souvent, les informations sont mises à la disposition d'un serveur distant, mais les modalités de cette collecte peuvent varier.

58. Certains appareils IDO disposent d'une connexion directe à un réseau public de communications avec une carte SIM cellulaire. D'autres peuvent être dotés d'une connexion indirecte à un réseau public de communications, par exemple par l'utilisation du WIFI ou la transmission d'informations à un autre dispositif par une connexion point à point (par exemple, par Bluetooth). L'autre dispositif peut, par exemple, être un smartphone ou un portail dédié, qui peut ou non prétraiter les informations avant de les envoyer au serveur.

59. Les dispositifs IDO peuvent être programmés par le fabricant afin de toujours transmettre les informations collectées, tout en mettant d'abord les informations en cache au niveau local, par exemple jusqu'à ce qu'une connexion soit disponible.

60. En tout état de cause, le dispositif IDO, lorsqu'il est connecté (directement ou indirectement) à un réseau public de communications, serait lui-même considéré comme un équipement terminal. Le fait que les informations soient transmises en continu ou mises en cache aux fins d'une communication intermittente ne change rien à la nature de ces informations. Dans les deux cas, l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'appliquerait étant donné qu'il existe une «obtention de l'accès» du fait de l'instruction inscrite dans le code du dispositif IDO d'envoyer les données stockées dynamiquement au serveur distant.

([29]) Les fournisseurs d'accès à l'internet utilisent le NAT de classe transporteur (*Carrier-grade NAT* ou CGNAT) pour maximiser l'utilisation de l'espace d'adressage IP limité. Cela permet de regrouper un certain nombre d'abonnés sous la même adresse IP publique.

([30]) L'avis 9/2014 du groupe de travail «article 29» mentionne un certain nombre d'exemples de situations dans lesquelles l'accord pourrait ne pas être nécessaire.

3.5 Identificateur unique

61. Un outil courant utilisé par les entreprises est la notion d'«identificateurs uniques» ou d'«identificateurs persistants». Ces identificateurs peuvent découler de données à caractère personnel persistantes (nom et prénom, adresse électronique, numéro de téléphone, etc.), qui sont hachées sur l'appareil de l'utilisateur, collectées et partagées entre plusieurs responsables du traitement afin d'identifier une personne de manière unique au moyen de différents ensembles de données [données d'utilisation collectées au moyen de l'utilisation d'un site web ou d'une application, données de gestion de la relation client (CRM) relatives à un achat ou à un abonnement en ligne ou hors ligne, etc.]. Sur les sites internet, les données à caractère personnel persistantes sont généralement obtenues dans le cadre de l'authentification ou de l'abonnement à des bulletins d'information.

62. Comme indiqué précédemment, le fait que des informations soient saisies par l'utilisateur n'empêcherait pas l'application de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques en ce qui concerne le stockage, étant donné que ces informations sont stockées temporairement sur l'équipement terminal avant d'être collectées.

63. Dans le cadre de la collecte d'un «identificateur unique» sur des sites web ou des applications mobiles, l'entité qui collecte les données demande au navigateur (par la distribution d'un code côté client) d'envoyer ces informations. Il s'agit donc d'une «obtention de l'accès» et l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique.