MARS 2017
UCOPIA DOCUMENT

LIVRET JURIDIQUE

La réponse aux obligations légales pour les organisations offrant un accès à l'internet au public en France et dans les Etats membres de l'Union Européenne.

SOMMAIRE

UCOPIA
TURN YOUR WI-FI UP

1 \ CONTEXTE

Offrir un accès à l'internet au public n'a rien d'anodin.

Depuis une loi n°2006-604 du 23 janvier 2006 relative à la lutte contre le terrorisme, les cafés, hôtels, cybercafés, restaurants, aéroports, mais aussi toutes les personnes qui offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont, en effet, tenues de conserver un certain nombre de données dites de trafic.

Le présent livre a notamment pour but d'alerter ces personnes qui, faute d'avoir conscience des obligations auxquelles elles sont tenues, offrent, bien souvent à leurs clients, une connexion permettant une communication à l'internet sans avoir pris le soin de mettre préalablement en place le dispositif qui leur permettra de transmettre, à qui de droit, les informations qu'elles étaient pourtant tenues de conserver.

Parce que ces différentes obligations sont notamment assorties de sanctions pénales, il apparaît nécessaire de les détailler.

Une directive 2006/24/CE en date du 15 mars 2006, qui a été invalidée en 2014 par la Cour de Justice de l'Union Européenne, a également contraint l'ensemble des Etats membres de l'Union européenne à adopter une loi obligeant les prestataires de services de communications électroniques accessibles au public et de réseaux publics de communication de conserver les données relatives aux communications pour une durée comprise entre 6 et 24 mois.

Le présent livre indique donc quelles sont les législations nationales qui ont transposé cette directive, quelles durées de conservation elles imposent et quelles ont été les conséquences internes de l'invalidation de cette directive prononcée par un arrêt de la CJUE en date du 8 avril 2014, avant qu'elle ne soit précisée par un arrêt en date du 21 décembre 2016 de cette même Cour.

Ce guide évoquera également les grandes lignes du règlement européen sur la protection des données qui entrera en vigueur dans les Etats membres de l'Union européenne, sans qu'une transposition ne soit nécessaire, à compter de mai 2018.

Sadry PORLON, Avocat au Barreau de Paris.

Docteur en droit, il est également chargé d'enseignement en école de commerce et en école d'ingénieur, notamment en droit des médias et de la communication ainsi qu'en droit du commerce électronique et du multimédia.

2 \ ZOOM

Le cas français, ce que vous devez savoir sur la loi contre le terrorisme & autres dispositions légales en 5 points.

	Loi contre le terrorisme & autres dispositions légales	**Loi HADOPI**
L'opérateur de communications électroniques est tenu de conserver…	- Les informations permettant d'identifier l'utilisateur - Les données relatives aux équipements et terminaux utilisés - Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication - Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs - Les données permettant d'identifier le ou les destinataires de la communication (Décret n°2006-358 du 24 mars 2006, article R. 10-13 du CPCE)	
L'opérateur de communications électroniques ne doit pas conserver…	« le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications » (Article L. 34-I-V du CPCE)	
Les sanctions en cas de non respect de l'obligation de conservation des données sont…	Un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques et 375.000 euros pour les personnes morales. (Article L. 39-3 du CPCE)	
La durée de conservation des données est…	D'un an pour le cas de la conservation des données relatives au trafic lorsqu'il s'agit de la recherche, de la constatation et de la poursuite des infractions. (Le décret du 24 mars 2006 prévoit des durées de conservations variables en fonction des finalités).	
Des données à délivrer aux personnes habilitées à les recevoir sous peine de sanctions pénales…	Les données conservées par l'opérateur de communications électroniques ne peuvent être transmises qu'à des personnes habilitées parmi lesquelles : - L'officier de police judiciaire au cours d'une enquête de flagrance - le Procureur de la République ou l'officier de police judiciaire sur autorisation du procureur et au cours d'une enquête préliminaire - le juge d'instruction ou l'officier de police judiciaire par lui commis au cours de l'instruction - les agents individuellement habilités des services de police et de gendarmerie, spécialisés dans la prévention des actes de terrorisme (Articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale ainsi que l'article L. 34-1-1 du CPCE) L'article L. 39-4 du CPCE précise que : « sera puni de trois mois d'emprisonnement et de 30.000 euros d'amende ou de l'une de ces deux peines seulement quiconque aura, sans raison valable, refusé de fournir les informations ou documents ou fait obstacle au déroulement de l'enquête ».	La commission de protection des droits de la HADOPI peut demander à l'opérateur de communications électroniques de lui remettre : - nom de famille, prénoms ; - Adresse postale et adresses électroniques ; - Coordonnées téléphoniques ; - Adresse de l'installation téléphonique de l'abonné (Décret n° 2010-236 du 5 mars 2010 en son article 2) « Est puni de l'amende prévue pour les contraventions de cinquième classe (soit 1.500 euros) le fait de contrevenir aux dispositions de l'article R. 331-37 » à savoir, pour l'opérateur de communications électroniques, de ne pas communiquer les données à caractère personnel et les informations mentionnées au 2° de l'annexe du décret n° 2010-236 du 5 mars 2010 qui lui seront réclamées. (Article R. 331-38 du décret n° 2010-872 du 26 juillet 2010)

Transposition de la directive 2006/24/CE, invalidation de cette dernière par la CJUE et durées de conservation des données imposées par les Etats membres de l'Union Européenne

Même si la France, par le biais du décret n°2006-358 du 24 mars 2006 relatif à la conservation des communications électroniques qui faisait suite à la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, n'a pas eu à transposer la directive au motif que son droit interne était d'ores et déjà conforme, les 26 autres pays de l'Union Européenne devaient y procéder.

La directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE définit les règles et les procédures de conservation des données personnelles ainsi que des registres d'appels téléphoniques que doivent respecter les prestataires de services de communications électroniques accessibles au public et de réseaux publics de communication.

Cette directive exige la conservation des données relatives au trafic générées par l'utilisation des services de communication électronique pendant une période allant de six mois à deux ans .

Elle prévoit que la durée maximale de conservation de ces données peut être prolongée par un État membre s'il est « confronté à des circonstances particulières justifiant une prolongation, pour une période limitée » et à la condition que cette prolongation soit notifiée à la Commission, laquelle peut, dans un délai de six mois suivant la notification, approuver ou rejeter la prolongation. Si la durée maximale peut être prolongée, aucune disposition ne prévoit la réduction de la durée de conservation en deçà de six mois.

L'obligation de conservation s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

En vertu de l'article 5 de la directive, les catégories de données à conserver sont :
a) les données nécessaires pour retrouver et identifier la source d'une communication
b) les données nécessaires pour identifier la destination d'une communication
c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication
d) les données nécessaires pour déterminer le type de communication
e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel
f) les données nécessaires pour localiser le matériel de communication mobile

Cette directive devait impérativement être transposée avant le 15 septembre 2007 par les Etats membres de l'Union européenne.

Le tableau qui suit vise à faire apparaître la durée de conservation des données qu'imposent les pays de l'Union européenne qui avaient, comme la France, l'obligation de transposer la directive.

Il fait également état des pays dans lesquels des décisions de justice ont déclaré inconstitutionnelles les lois votées par les parlements nationaux qui transposent la directive.

Il est utile de préciser qu'une législation sur la conservation des données existe également dans des pays qui ne font pas partie de l'Union européenne, mais de l'Espace Economique Européen (EEE) parmi lesquels l'Islande, le Liechtenstein et la Norvège .

Nous allons donc voir ce qu'ont décidé les Etats membres concernant la durée de l'obligation de conservation des données relatives au trafic et des données de localisation qu'ils étaient tenus d'imposer aux opérateurs de communications électroniques opérant sur leur territoire.

---

[1] L'article 6 de la directive dispose que : « Les États membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication ».

L'opérateur de communication électronique qui souhaite fournir un accès à l'Internet au public dans l'un des 27 pays membres de l'Union européenne et plus particulièrement dans ceux qui, à l'heure actuelle, ont transposé la directive 2006/24/CE, doit, en effet, s'assurer de disposer des outils techniques permettant une collecte des données relatives au trafic et des données de localisation des internautes répondant précisément aux préconisations de la loi transposant la directive en droit interne et ne pas oublier que ces données ne devront être communiquées qu'à un nombre restreint d'autorités habilitées à se les faire délivrer.

Cependant, et pour rappel, le 8 avril 2014, la Cour de Justice de l'Union Européenne (ci-après CJUE) a invalidé intégralement la directive sur la conservation des données de connexion (directive 2006/24/CE) sur la rétention des données de connexion suite à deux recours préjudiciels portant sur deux affaires conjointes Digital Rights Ireland Ltd n°C-293/12 (Irlande) et Karntner Landesregierung n°C-594/12 (Autriche).

La demande présentée par la High Court (affaire C 293/12) concernait un litige opposant Digital Rights Ireland Ltd au Minister for Communications, Marine and Natural Resources, au Minister for Justice, Equality and Law Reform, au Commissioner of the Garda Síochána, à l'Irlande ainsi qu'à l'Attorney General au sujet de la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques.

La demande présentée par le Verfassungsgerichtshof (affaire C 594/12) est relative à des recours en matière constitutionnelle introduits devant cette juridiction respectivement par la Kärntner Landesregierung (gouvernement du Land de Carinthie) ainsi que par MM. Seitlinger, Tschohl et 11 128 autres requérants au sujet de la compatibilité de la loi transposant la directive 2006/24 dans le droit interne autrichien avec la loi constitutionnelle fédérale (Bundes-Verfassungsgesetz).

La Cour de Justice de l'Union Européenne a considéré la directive 2006/24/CE comme contraire aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne qui a valeur contraignante depuis le traité de Lisbonne entré en vigueur en 2009.

La CJUE ne conteste pas la principe et l'utilité de la conservation stricte des données aux fins de permettre aux autorités judiciaires de disposer d'un accès à celles-ci pour défendre l'intérêt général à savoir la lutte contre la criminalité grave et de garantir la sécurité publique, mais les tempère en indiquant qu'une telle ingérence ne devrait être envisageable qu'à la condition que les mesures prévues soient déterminées de manière proportionnée.

Les principaux écueils de la directive mises en avant par la CJUE dans son arrêt sont que :

1. L'obligation de conservation concerne toute personne, tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic, sans différenciation, limitation ou exception opérées en fonction de l'objectif de lutte contre les infractions graves ; (pt 59)

2. L'accès ouvert aux données collectées est trop large et est encadré de manière insuffisante. Il se borne, en effet, à renvoyer de manière générale aux « infractions graves » définies par chaque Etat membre dans son droit interne ; (pt 60)

3. L'accès ne fait pas l'objet d'un contrôle préalable par une juridiction ou une autorité indépendante ; (pt 61)

4. Aucune durée précise de conservation n'est imposée aux Etats, seule une période de 6 mois à 24 mois est prévue sans qu'il ne soit fait de distinction entre les personnes ni entre les infractions concernées (pt 63 et 64).

5. La directive ne prévoit pas de garanties suffisantes permettant d'assurer une protection efficace des données contre les risques d'abus et d'utilisation illicite (pt 66 et 67).

6. La directive n'impose pas que les données recueillies soient conservées sur le territoire de l'Union Européenne afin de garantir pleinement le contrôle du respect des exigences de protection et de sécurité par une autorité indépendante comme l'exige la Charte des droits fondamentaux de l'Union européenne (pt 68).

7. La directive ne garantit pas la destruction irrémédiable des données au terme de leur durée de conservation par les services de communications électroniques (pt 67)

---

[2] La loi islandaise est une loi sur les télécommunications 81/2003 telle que modifiée en avril 2005.

Au Liechtenstein, il s'agit d'une loi sur les télécommunications de 2006. En Norvège, une loi a été votée le 5 avril 2011.

Concernant les conséquences de cet important arrêt de la CJUE, il convient de noter que l'invalidité de la directive n'affecte pas directement les législations nationales des Etats membres, mais que les juridictions nationales peuvent être appelées à se prononcer sur la conformité des lois nationales au regard des droits fondamentaux sur la base de l'analyse ainsi livrée par la Cour de justice de l'Union européenne.

L'invalidité de la directive ne rendait donc pas mécaniquement les dispositions nationales contraires au droit de l'Union européenne.

Se posait alors la question de savoir si Commission et le Parlement européen allaient être amenés à réécrire la directive en tenant, cette fois, compte des remarques mises en avant par la CJUE à l'encontre de la directive invalidée ou si les corrections se feraient au niveau national.

Pour information, dès le 12 mars 2015, le commissaire chargé des Affaires intérieures Dimitris Avramopoulos, a indiqué, lors d'une conférence de presse que la Commission européenne ne présentera pas de nouvelle directive en matière de rétention de données, en remplacement de la directive invalidée par la Cour de justice de l'UE en avril 2014.

Il précisait ceci : « Je veux être clair : il n'aura pas de nouvelle directive sur la rétention des données. La Commission n'a pas l'intention de présenter une nouvelle initiative législative. Ces derniers mois, plusieurs Etats membres ont introduit ou sont en train de préparer leurs propres initiatives. La position de la Commission est très claire là-dessus ».

Nous verrons donc dans le tableau ci-dessous que certains Etats membres de l'Union européenne n'ont pas tardé à en tenir compte en prononçant l'inconstitutionnalité de leurs législations nationales et que d'autres en sont au stade où ils proposent à leurs gouvernements une nouvelle loi qui tirera les enseignements des conclusions de l'arrêt de la CJUE du 8 avril 2014.

Pour rappel, la législation française en matière de conservation des données est issue du décret n°2006-358 du 24 mars relatif à la conservation des communications électroniques qui faisait suite à la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

Les dispositions françaises prévues aux articles L. 34-1 du Code des postes et des communications électroniques (ci-après CPCE) concernant les enquêtes judiciaires et L. 34-1-1 du CPCE concernant les enquêtes administratives en matière de conservation des données ainsi qu'aux articles R. 10-13 et suivants du CPCE sont donc toujours applicables, même si l'invalidation de la directive implique que les Etats membres s'interrogent sur l'impact de cette invalidation sur leur législation nationale, et ce d'autant depuis un important et récent arrêt de la CJUE en date du 21 décembre 2016.

Ainsi l'arrêt de la CJUE rendu le 21 décembre 2016 (Tele2 Sverige AB/Post-Och telestyrelsen (C-203/15) et Secretary of State for the Home Department/Tom Watson e.a. (C-698/15) prend le contrepied des conclusions de l'Avocat général Saugmandsgaard Øe en date du 19 juillet 2016.

Cet arrêt se veut un complément sur l'interprétation qu'il convenait de faire, notamment au niveau national, de l'arrêt Digital Rights Ireland Ltd (C-293/12 et C-594/12) en date du 8 avril 2014, lequel avait procédé à l'invalidation intégrale et rétroactive de la directive 2006/24/CE concernant la rétention des données de communications électroniques.

Les deux affaires tranchées le 21 décembre 2016 consistaient donc dans l'analyse de l'obligation générale imposée aux fournisseurs de services de télécommunications en Suède, d'une part et au Royaume-Uni, d'autre part de conserver les données relatives aux communications électroniques.

Il s'agit pour la CJUE de préciser l'interprétation à apporter dans un contexte national à l'arrêt Digital Rights Ireland Ltd.
Dans la première affaire, Tele2 Sverige AB, suite à l'invalidation de la directive, a notifié aux autorités qu'elle cesserait de conserver les données relatives aux communications électroniques. Compte tenu du fait qu'il lui était enjoint de conserver ces données, elle a décidé d'introduire un recours juridictionnel devant le Tribunal administratif puis devant la Cour d'Appel administrative de Stockholm.

Cette cour de renvoi a alors saisi la CJUE afin que celle-ci se prononce sur la question de savoir si l'obligation généralisée de conservation des données relatives aux communications électroniques est compatible, eu égard à l'arrêt précité en date du 8 avril 2014, avec l'article 15 de la directive 2002/58/CE et à la lumière des articles 7, 8 et 52 § 1 de la charte des droits fondamentaux de l'Union.

Dans l'autre affaire, spécifique au Royaume-Uni, des parlementaires anglais ont décidé de former un recours juridictionnel contre l'article 1er de la loi DRIPA (Data retention and investigatory Powers Act) en invoquant son incompatibilité avec les articles 7 et 8 de la Charte ainsi qu'avec l'article 8 de la CEDH.

Par son arrêt en date du 21 décembre 2016, la CJUE confirme que les mesures nationales en cause relèvent du champ d'application de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002.

La Cour insiste ensuite sur le nécessaire respect du principe de proportionnalité dans la collecte des données, constate que les législations nationales den cause prévoient « une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception » (§ 97).

Elle constate s'agissant de la conservation que les données conservées prises dans leur ensemble sont susceptibles de permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données ont été conservées (§ 99).

Elle précise que la directive ne s'oppose pas à une réglementation nationale imposant une conservation ciblée des données à des fins de lutte contre la criminalité grave, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

Elle ajoute que toute réglementation nationale facilitant la conservation des données doit être claire et précise et prévoir des garanties suffisantes afin de protéger les données des risques d'abus.

Elle exige que la réglementation nationale subordonne l'accès des autorités nationales compétentes aux données conservées, sauf en cas d'urgence, à un contrôle préalable effectué par une juridiction ou une entité indépendante (§ 119), que lesdites autorités en informe les personnes concernées, que les données soient conservées sur le territoire de l'Union et qu'elles soient détruites au terme de la durée de leur conservation (§ 122).

En somme, l'enseignement de cet arrêt tient au fait qu'il impose au niveau national :

- Que la conservation des données ne soit pas généralisée et indifférenciée (et donc qu'elle soit ciblée)

- Que l'accès aux données conservées soit limité aux seules fins de lutte contre la criminalité grave

- Que ce même accès soit subordonné à un contrôle préalable par une juridiction ou une autorité nationale

- Que les données soient conservées sur le territoire de l'Union

Le 17 janvier 2017, le député français Lionel TARDY a interrogé le ministre de la justice sur la portée de cet arrêt.

Le 22 avril 2014, ce même député avait déjà interrogé la garde des sceaux de l'époque (question n°54368) sur la portée de l'arrêt Digital Rights Ireland Ltd (C-293/12 et C-594/12) en date du 8 avril

2014 sur les procédures initiées au niveau national, tant au niveau pénal, que civil qu'administratif, visant à solliciter des opérateurs de communications électroniques la transmission des données sur l'activité de leurs utilisateurs.

Il lui avait été répondu, plus de 2 ans plus tard, soit le 7 juin 2016 que la CJUE n'avait pas invalidé le principe de la conservation des données et cet arrêt était sans impact sur les dispositions nationales, notamment sur l'article L. 34-1 du Code des postes et des communications électroniques (CPCE), dans la mesure où ces dernières sont antérieures à la directive invalidée et que : « La législation française apporte des garanties supérieures à celles prévues par le directive invalidée en matière de protection des données et de contrôle des demandes d'accès aux données, dès lors, notamment, que les données de connexion sont conservées sur le territoire français et soumises au contrôle de la Commission national de l'informatique et des libertés, que des sanctions pénales sont encourues en cas de consultations indues et que les personnes habilitées à consulter ces données sont déterminées par la loi ».

Elle concluait en indiquant qu' : « Enfin, l'arrêt du 8 avril 2014 n'emporte pas de conséquences directes sur les mesures mises en œuvre par les autorités nationales sur le fondement de la directive 2006/24/CE, ainsi que l'a admis le groupe de travail de l'article 29, qui réunit les autorités de protection des données de l'Union européenne, dans son opinion WP220 du 1er août 2014 ».

Le député soutient désormais dan sa nouvelle question en date du 17 janvier 2017 que : « Dans une réponse formulée le 7 juin 2016 à sa question n°54368, M. le garde des sceaux avait estimé que cet arrêt était sans impact sur les dispositions nationales (…) Or, l'arrêt Tele2 vient infirmer une telle interprétation (…) Pour la CJUE, les mesures nationales de conservation de données par les fournisseurs de services de communication électroniques relèvent bien du champ d'application du droit de l'Union. Partant de là, la CJUE, sans rejeter le principe même d'une conservation de données de connexion, vient rappeler quelques conditions intangibles devant être scrupuleusement respectées par les législations nationales. (…) pour la CJUE, seule la lutte contre la criminalité grave est susceptible de justifier l'ingérence résultant d'une réglementation nationale prévoyant la conservation des données relatives au trafic et des données de localisation. Par ailleurs, elle conditionne l'accès aux données conservées au respect de plusieurs exigences.
Premièrement, l'accès doit être subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, ce qui pose la question de la validité des demandes formulées au titre 1) d'enquêtes diligentées sous l'autorité du Parquet et 2) du droit de communication de l'administration pour des données conservées par les fournisseurs de services de communications électroniques dans la mesure où il n'existe à ce jour aucun contrôle préalable des demandes de l'administration – hormis pour les sujets relevant de l'accès administratif aux données de connexion soumis au contrôle de la CNCTR.
Deuxièmement, les personnes dont les données conservées ont été demandées par les autorités doivent être informées par ces dernières, dès lors que cette communication n'est pas susceptible de compromettre les enquêtes menées. Enfin la conservation des données doit avoir lieu sur le territoire de l'Union, ce qui pose la question de la validité des demandes portant sur des données conservées hors de l'Union par de grands acteurs d'internet ».

Il conclut sa question de la façon suivante : « Par conséquent, il souhaite donc obtenir des précisions quant à la portée de cet arrêt Tele2 sur les procédures initiées au niveau national visant à solliciter de la part des fournisseurs de services de communications électroniques, la transmission de données sur l'activité de leurs utilisateurs. En particulier, dans la mesure où le non respect des principes rappelés par la CJUE fait peser un risque sur ces procédures, il souhaite connaître les moyens qu'il compte mettre en œuvre pour mettre en conformité notre droit national, notamment pour ce qui concerne le droit de communication de l'administration, avec les prescriptions formulées par la CJUE ».

Eu égard à l'arrêt de la CJUE en date du 21 décembre 2016 qui précise l'interprétation qui doit être faite de l'invalidation de la directive au niveau national, on peut s'attendre, à court ou moyen terme, à ce qu'une loi nationale vienne corriger en France les absences mis en avant par le député Lionel TARDY dans sa question écrite n°102017 en date du 17 janvier 2017.

Le fait qu'elle intègre les différentes préconisations issues des arrêts précités permettrait à la France d'éviter :

- que les prévenus ou accusés sur la base de renseignements obtenus auprès des opérateurs sur la base de la législation actuelle soulèvent à leur profit l'irrégularité des poursuites pénales engagées en raison de l'invalidité de la loi française eu égard aux arrêts de la CJUE en date des 8 avril 2014 et 21 décembre 2016

- que des recours devant le Conseil d'Etat ne soient pas initiés afin de voir abroger la disposition nationale jugée trop générale

- que les opérateurs de communications électroniques qui collectent les données n'opposent une fin de non-recevoir aux demandes de transmission des données stockées qui leur seraient soumises par les autorités policiers et judiciaires

- que ces mêmes fournisseurs de services de communication électronique refusent purement et simplement de collecter lesdites données au motif que la loi qui leur impose de le faire ne serait pas conforme (à l'image de ce qu'à pu faire Tele2 en Suède)

- que les utilisateurs de services de communication au public en ligne réclament la destruction des données collectées par le responsable du traitement en raison d'un motif légitime de ne pas figurer dans lesdits fichiers

- que le Premier ministre modifie, d'office ou sur demande d'un tiers, les dispositions réglementaires du Code des postes et communications électroniques régissant la conservation des données afin de le mettre en conformité avec les raisons de la censure de la directive par les arrêts précités.

Il appartient, de façon plus générale, à la lumière de cet arrêt du 21 décembre 2016, aux juridictions nationales à l'origine du renvoi préjudiciel de résoudre individuellement les affaires qui lui avaient été soumises conformément à la décision de la Cour ; étant précisé que les autres juridictions nationales des pays de l'Union seraient tenues de la même manière dans l'hypothèse où elles devaient être saisies d'une problématique similaire à celle de l'arrêt du 21 décembre 2016.

Pays	Textes de loi transposant la directive	Durées de conservation des données fixée dans la législation nationale	Remarques
Allemagne	Loi de révision sur la surveillance du secteur des télécommunications et d'autres mesures d'enquête ainsi que sur la mise en œuvre de la directive 2006/24/CE Date de publication 31/12/2007 Entrée en vigueur : 01/01/2008	12 mois à compter de la date de la communication. Dans l'attente d'une nouvelle loi transposant la directive 2006/24/CE fixant éventuellement une durée différente	La Cour constitutionnelle fédérale allemande a déclaré inconstitutionnelle certaines dispositions de la loi allemande transposant la directive par un arrêt en date du 2 Mars 2010 le 27 octobre 2011, la Commission a formellement invité l'Allemagne à prendre, dans un délai de deux mois, des mesures permettant d'assurer le plein respect des règles de l'UE relatives à la conservation des données Le 26 mars 2012, la Commission a averti l'Allemagne qu'elle saisira la Cour de Justice de l'Union Européenne (ci-après CJUE) afin que cette dernière prononce des amendes à son égard. Compte tenu du fait que les autorités allemandes n'ont pas faire savoir comment ni quand elles entendaient adopter une nouvelle législation transposant pleinement la directive 2006/24/CE, la Commission a décidé de porter l'affaire devant la CJUE La Commission a notamment proposé à la Cour d'infliger une astreinte de 315 036,56 euros par jour de retard jusqu'à ce que l'Allemagne se mette en conformité avec le droit de l'Union. Tenant compte des enseignements de l'arrêt de la CJUE en date du 8 avril 2014, un nouveau projet de loi allemand présenté en 2015 prévoit notamment que les données doivent être conservées en Allemagne uniquement ainsi que la conservation obligatoire des données issues des téléphones portables et des adresses IP d'ordinateurs pendant 10 semaines. Cette proposition de loi allemande sur la conservation des données sera présentée au gouvernement fédéral allemand (Bundestag) en juin 2015. L'Allemagne est, avec le Luxembourg, un des premiers pays de l'Union européenne à soumettre une nouvelle loi sur la conservation des données depuis que la Cour de justice de l'Union a invalidé la directive de 2006.
Autriche	Loi fédérale modifiant la loi sur les télécommunications de 2003 Date de publication : 18/05/2011 Entrée en vigueur : 19/05/2011	6 mois à compter de la date de la communication	L'arrêt de la CJUE en date du 8 avril 2014 a tranché en faveur de l'invalidité de la directive 2006/24/CE sur la base d'un recours préjudiciel émanant notamment de la cour constitutionnelle autrichienne. Le 27 juin 2014, la Cour constitutionnelle autrichienne a déclaré inconstitutionnelle la plupart des parties de la loi autrichienne sur la conservation des données.

Belgique	Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques	Douze mois à partir de la date de la communication pour la recherche et la poursuite de faits punissables.	Le texte se fonde sur les dispositions de la loi du 30 juillet 2013 annulée par la cour constitutionnelle belge dans un arrêt en date du 11 juin 2015 (n°84/2015) se fondant sur l'arrêt de la CJUE en date du 8 avril 2014. L'accès aux données est limité en fonction du degré de gravité de l'infraction. Pour les petites infractions (6 mois), pour les enquêtes pour terrorisme (12 mois). Le législateur délimite clairement qui a accès aux données, les modalités de traitement des données consultées et prévoit des garanties pour les professions soumises au secret professionnel, avocats, médecins, journalistes).
Bulgarie	Loi sur les communications électroniques Date de publication: 02/03/2010 Entrée en vigueur: 10/05/2010 Ordonnance N°40 du 7 Janvier 2008 propres à certaines catégories de données et la façon dont elles sont stockés et mises à disposition par les entreprises fournissant des réseaux de communications électroniques et / ou des services dans l'intérêt de la sécurité nationale et de la détection de la criminalité Date de publication: 29/01/2008 Entrée en vigueur: 01/02/2008	12 mois à compter de la date de la communication. Les données auxquelles l'accès a été accordé peuvent être conservées six mois de plus sur demande	Une action relative à la conservation des données a été introduite devant la Cour administrative suprême de Bulgarie (arrêt n°13627 du 11 décembre 2008) Cela a entrainé une révision de la loi de transposition. Le 12 mars 2015, la loi de conservation des données bulgares a été, de nouveau, déclarée incompatible avec la constitution en se basant en partie sur l'arrêt de la CJUE en date du 8 avril 2014.
Chypre	La loi sur la conservation des données de télécommunications pour les crimes graves. Date de publication 31/12/2007 Entrée en vigueur : 31/12/2007	6 mois à compter de la date de la communication	Plusieurs affaires relatives à la conservation des données ont été portées devant la Cour constitutionnelle chypriote (affaires n°65/2009, 78/2009 et 15.2010-22.2010 du 1er février 2011). La Cour a jugé inconstitutionnelles les ordonnances des tribunaux rendues en vertu de la loi de transposition La loi de transposition reste néanmoins valable
Danemark	Première, deuxième et troisième ordonnance sur les fournisseurs de réseaux de communications électroniques et de services de communications électroniques d'enregistrement et le stockage de l'information sur le trafic Date de publication : 13/10/2006 Entrée une vigueur: 15/09/2007	12 mois à compter de la date de la communication	Le Parlement danois a commandé une étude sur la légalité des ordonnances sur la conservation des données, compte tenu de l'arrêt de la CJUE en date du 8 avril 2014.

Espagne	Loi n°25/2007 de conservation des données sur les communications électroniques et des réseaux de communications publics Date de publication : 19/10/2007 Entrée en vigueur: 08/11/2007	12 mois à compter de la date de la communication Une autorité compétente peut, après consultation des opérateurs de télécommunications électroniques, réduire cette durée de conservation à 6 mois ou au contraire l'augmenter à 24 mois pour certaines données ou catégories de données	
Estonie	Loi sur les communications électroniques et la santé publique Date de publication et d'entrée en vigueur : 07/12/2007	12 mois à compter de la date de la communication	
Finlande	Loi d'obligation d'identification et de stockage des données / Loi sur la vie privée dans les communications électroniques Entrée en vigueur : 05/06/2008	12 mois à compter de la date de la communication	La Finlande n'impose pas aux petits opérateurs l'obligation de conserver les données au motif que les coûts que cela représente tant pour le fournisseur que pour l'État dépasseraient les bénéfices pour les services répressifs et la justice pénale
Grèce	Loi de conservation des données générées ou traitées en collaboration avec les réseaux publics de communications, l'utilisation de systèmes de surveillance, de réception ou d'enregistrement audio ou vidéo dans les lieux publics et dispositions connexes Date de publication : 21/02/2011	12 mois à compter de la date de la communication	
Hongrie	Loi de 2003 sur les communications électroniques Date de publication : 13/12/2003 Loi de 2007 modifiant la loi sur les communications électroniques	6 mois pour les appels téléphoniques infructueux et 12 mois pour toutes les autres données	Une action a été introduite le 2 juin 2008 par l'union hongroise des libertés civiles devant la Cour constitutionnelle hongroise. Elle est actuellement pendante.
Italie	Loi de mise en œuvre de la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou réseaux de communications publics et modifiant la directive 2002/58/CE Date de publication : 18/06/2008 Décret législatif n°7 du 18 janvier 2015 confirmé par la loi n°43 du 17 avril 2015.	12 mois à compter de la date de la communication	

Irlande	Loi sur la conservation des données de communications de 2011 Date de publication: 28/01/2011	24 mois pour les données de téléphonie fixe et mobile 12 mois pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet	Le 11 juin 2012, la High Court of Ireland a adressé à la Cour de Justice de l'Union Européenne, une demande de décision préjudicielle portant sur la directive 2006/24/CE enregistrée sous le numéro d'affaire C-293/12. La réponse de la CJUE est intervenue dans le cadre du désormais célèbre arrêt du 8 avril 2014 ayant débouché sur l'invalidation de la directive.
Lettonie	Modifications de la Loi sur les communications électroniques du 17/11/2004 Date de publication: 24/05/2007 Entrée en vigueur: 07/06/2007 Procédures obligeant les opérateurs de communication électronique à recueillir et à conserver des informations statistiques sur les données et à les délivrer sur demande aux autorités d'enquête avant le procès, aux exploitants d'urgence, aux autorités de sécurité nationale et au ministère public selon ordonnances du tribunal Date de publication: 07/12/2007 Entrée en vigueur: 08/12/2007	18 mois à compter de la date de la communication	
Lituanie	Loi lituanienne sur les communications électroniques Date de publication: 29/11/2008 Entrée en vigueur: 15/03/2009	6 mois à compter de la date de la communication	
Luxembourg	Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics. Date de publication: 29/07/2010 Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle Date de publication: 29/07/2010	6 mois à compter de la date de la communication	Suite à l'arrêt de la CJUE en date du 8 avril 2014, le ministre luxembourgeois de la Justice a demandé un avis de la Commission Nationale pour la Protection des données (ci-après CNPD), l'autorité de protection des données au Luxembourg, en vue d'évaluer la conformité de la législation luxembourgeoise avec les points soulevés par la CJCE. Le 13 mai 2014, la CNPD a publié son avis avec la recommandation principale de redéfinir la condition pour lutter contre les crimes graves et organisés et le terrorisme par une qualification et incrimination plus appropriée des faits qui font l'objet de l'enquête. Le 7 Janvier 2015, le ministère luxembourgeois de la Justice a déposé le projet de loi n ° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques afin de se conformer à l'arrêt de la CJUE et de combler la lacune créée par l'invalidation de la directive précitée. Après toute une série de consultations, le Conseil d'Etat luxembourgeois a rendu le 7 février 2017 son avis concernant une série d'amendements gouvernementaux apportés sur une version du texte précité en date du 8 décembre 2016.

Malte	Loi modificative sur la protection des données de 2008 (LN. 198) Date de publication 29/08/2008 Loi sur les communications électroniques régulation) (LN. 198) (CAP 399) Date de publication : 29/08/2008	12 mois pour toutes les données relatives à la téléphonie fixe, mobile et par l'internet 6 mois pour toutes les données relatives à l'accès à l'internet et au courrier électronique par l'internet	
Pays-Bas	Loi du 18 Juillet 2009 modifiant la loi sur les télécommunications et les infractions économiques en relation avec la mise en œuvre de la directive 2006/24/CE du Parlement européen et du Conseil de l'Union européenne sur la rétention de données traitées dans le cadre avec la fourniture de services de communications électroniques et modifiant la directive 2002/58/CE (Loi sur la conservation des données de télécommunications)	12 mois à compter de la date de la communication	Une décision de la Cour de la Haye du 11 mars 2015 (C/09/48009/KG) Z1 14/1575) prononcée suite à un recours s'appuyant sur l'arrêt de la CJUE en date du 8 avril 2014 a déclaré inconstitutionnelle la loi sur la conservation des données.
Pologne	La réglementation du 28 Décembre 2009 du ministère des infrastructures concernant une liste complète de données et l'obligation de conservation à laquelle sont tenus les exploitants de réseaux publics de télécommunications ou de services de télécommunications accessibles au public. Loi du 24 avril 2009 modifiant la Loi sur les télécommunications du 16 juillet 2004 Décret du 22 Mars 2010 sur la façon de transmettre et de partager des données en cas de faillite d'un opérateur de réseau public de télécommunications ou un fournisseur de services de télécommunications accessibles au public	24 mois à compter de la date de la communication	
Portugal	Transposition en droit national de la directive 2006/24/CE du Parlement européen et du Conseil du 15 Mars, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques services ou des réseaux publics de communications Date de publication: 17/07/2008	12 mois à compter de la date de la communication	

République Tchèque	Loi n ° 247/2008 Coll. Modifiant la loi no 127/2005 Coll. Communications électroniques et modifiant certaines lois connexes Date de publication: 04/07/2008 Décret n ° 485/2005 Coll. La mesure du trafic et des temps de rétention des données de localisation et leur transmission aux organismes habilités à les utiliser Date de publication: 15/12/2005	De 6 à 12 mois à compter de la date de la communication. Déclarée inconstitutionnelle, elle devra faire l'objet d'une nouvelle transposition	Un arrêt de la Cour constitutionnelle tchèque du 22 mars 2011 a déclaré inconstitutionnelles la loi n°127/2005 et le décret n°485/2005. La République Tchèque examine actuellement comment procéder à une nouvelle transposition de la directive et le fera sans doute à l'aune des conclusions de l'arrêt de la CJUE en date du 8 avril 2014.
Roumanie	Loi sur la conservation de données générées ou traitées par les fournisseurs de services de communications électroniques ou réseaux de communications publics modifiant la loi n°506/2004 sur le traitement des données personnelles et la vie privée dans le secteur des communications électroniques (loi n° 298/2008) Date de publication : 21/11/2008 Loi n°82/2012 du 22 mai 2012 relative à la conservation des données générées ou traitées par les fournisseurs de réseaux de communications électroniques et par les services de communications électroniques destinés au public Date d'entrée en vigueur : 18 juin 2012	6 mois à compter de la date de la communication	Le 8 octobre 2009, la Cour constitutionnelle roumaine a jugé inconstitutionnelle la loi n° 298/2008 de transposition de la directive. le 27 octobre 2011, la Commission Européenne a formellement invité la Roumanie à prendre, dans un délai de deux mois, des mesures permettant d'assurer le plein respect des règles de l'UE relatives à la conservation des données Le 22 mai 2012, la Chambre des députés du Parlement roumain a adopté à une large majorité la loi relative à la conservation des données générées ou traitées par les fournisseurs de réseaux de communications électroniques et par les services de communications électroniques destinés au public Le 8 juillet 2014, la cour constitutionnelle roumaine a, de nouveau, indiqué que la nouvelle loi roumaine de transposition de la directive était inconstitutionnelle.
Royaume-Uni	Loi DRIPA (Sur la conservation des données et les pouvoirs d'enquête - Data retention and investigatory Powers Act) en date de 17 juillet 2014 Règlement de 2014 sur la conservation des données (Data Retention Regulations 2014)	Jusqu'à 12 mois à compter de la date de la communication	En 2015, des parlementaires anglais ont décidé de former un recours juridictionnel contre l'article 1er de la loi DRIPA (Data retention and investigatory Powers Act) en invoquant son incompatibilité avec les articles 7 et 8 de la Charte ainsi qu'avec l'article 8 de la CEDH. La Court of Appeal a procédé à un renvoi préjudiciel le 4 mai 2015 devant la CJUE, lequel renvoi a débouché sur l'arrêt du 21 décembre 2016 visé en introduction de ce guide.
Slovaquie	Loi n ° 654/2007 modifiant et complétant la loi n °610/2003 sur les communications électroniques	12 mois pour les données de téléphonie fixe et mobile, 6 mois pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet	Le 23 avril 2014, la cour constitutionnelle slovaque a suspendu l'application de la loi sur la conservation des données. La loi reste donc valable mais n'a aucun effet juridique contraignant. Les opérateurs de communication électronique ne sont donc, pour l'heure, plus tenus de conserver les données du trafic.

Slovénie	Règles relatives à la méthode de transmission des données de trafic détenues par services de la téléphonie mobile et les réseaux fixes de communications électroniques Date de publication: 14/12/2009 Entrée en vigueur: 13/01/2010 Loi modifiant la loi sur les communications électroniques Date de publication: 12/12/2006	8 mois pour les données relatives à l'internet. 14 mois pour les données de téléphonie	Le 3 juillet 2014, la cour constitutionnelle slovène a annulé la législation nationale de conservation des données du fait de son caractère inconstitutionnel en se basant notamment sur les conclusions de l'arrêt de la CJUE en date du 8 avril 2014.
Suède	Loi 2012/278 concernant la collecte des données sur les communications électroniques en application de la loi intelligence. Date de publication : 21 mars 2012 Date d'entrée en vigueur : 1er mai 2012	6 mois à compter de la date de la communication	La Suède a été déclarée coupable de manquement à l'obligation qui lui incombe en vertu de l'UE par la Cour de justice (C-185/09). En avril 2011, la Commission a intenté un second recours contre la Suède devant la Cour pour inexécution de l'arrêt rendu dans l'affaire C-185/09. La Suède s'exposait à une sanction financière en vertu de l'article 260 du traité sur le fonctionnement de l'Union Européenne à la suite de la décision de son parlement de retarder d'un an l'adoption de la loi de transposition. Le Parlement suédois a voté le 21 mars 2012 la Loi 2012/278 concernant la collecte des données sur les communications électroniques en application de la loi intelligence. Cette loi transpose la directive 2006/24/CE. Le 12 juin 2014, un groupe d'experts nommé par le ministre de la justice suédois a conclu que la législation suédoise est licite contrairement à la directive de 2006 invalidée par le directive dans le cadre de l'arrêt du 8 avril 2014. Suite à l'invalidation de la directive, la société Tele 2 a notifié aux autorités qu'elle cesserait de conserver les données relatives aux communications électroniques. Compte tenu du fait qu'il lui était enjoint de conserver ces données, elle a décidé d'introduire un recours juridictionnel devant le Tribunal administratif puis devant la Cour d'Appel administrative de Stockholm. Cette cour de renvoi a alors saisi, le 9 décembre 2015, la CJUE afin que celle-ci se prononce sur la question de savoir si l'obligation généralisée de conservation des données relatives aux communications électroniques est compatible, eu égard à l'arrêt précité en date du 8 avril 2014, avec l'article 15 de la directive 2002/58/CE et à la lumière des articles 7, 8 et 52 § 1 de la charte des droits fondamentaux de l'Union. L'arrêt de la CJUE en date du 21 décembre 2016 a débouché sur les conclusions développées en introduction de ce guide.

Suisse	Pas de transposition de la directive puisque la Suisse n'est pas un état membre de l'Union Européen. Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 6 octobre 2000 (actuellement en vigueur). Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 18 mars 2016 Entrée en vigueur (courant 2018)	Au moins 6 mois à compter de la date de la communication dans la LSCPT du 6 octobre 2000 6 mois à compter de la date de la communication dans la LSCPT du 18 mars 2016 qui entrera en vigueur en 2018.	Lors de sa séance du 22 mars 2017, le Conseil fédéral a mis en consultation les ordonnances de mise en œuvre de la nouvelle loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Comme pour la loi, l'objectif principal de ces ordonnances est d'éviter que des délinquants puissent échapper aux autorités de poursuite pénale en utilisant des technologies de communication nouvelles. La consultation durera jusqu'au 29 juin 2017. Les cinq ordonnances de mise en œuvre devraient ensuite entrer en vigueur en même temps que la loi, au début de 2018. Le Conseil fédéral fixera la date ultérieurement.

ENCADRE

UCOPIA WEB SERVICES :
L'opérateur de communication électronique : un responsable de traitements sur lequel pèse également des obligations liées au caractère personnel des données qu'il collecte.

Dans l'hypothèse où l'opérateur de communication électronique recueille des données présentant des risques particuliers d'atteinte aux droits et aux libertés, celui-ci devra veiller à obtenir une autorisation préalable de la Commission Nationale Informatique et Libertés (ci-après CNIL).

Dans le cas contraire, il pourra se contenter d'une déclaration normale du traitement, voire d'une déclaration simplifiée.

Le non-accomplissement de ces formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000 euros d'amende conformément à l'article 226-16 du Code pénal.

Tout responsable de traitement informatique de données personnelles doit également mettre en place des mesures de sécurité physiques, logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement.

Le non-respect de cette obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende est sanctionné par l'article 226-17 du Code pénal. Il devra également veiller à ce que seules les personnes autorisées puissent accéder aux données personnelles contenues dans les fichiers collectés (destinataires explicitement désignés et tiers autorisés – police, services des impôts).

Le responsable du fichier devra aussi s'assurer qu'il permet aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits de modification, de suppression et de retrait dudit fichier. Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 euros par infraction constatée et 3 000 euros en cas de récidive (Article 131-13 du Code pénal, Décret n°2005-1309 du 20 octobre 2005).

Le responsable du fichier devra respecter le principe dit de la finalité du traitement qui veut que les informations exploitées dans un fichier soient cohérentes par rapport à son objectif. Les informations collectées ne pourront pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.

Le non respect de cette règle est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende (Article 226-21 du Code pénal).

UCOPIA WEB SERVICES :

La question de collectes des données à caractère personnel afin d'en faire bénéficier à des partenaires dans un but commercial

Le responsable du traitement des données à caractère personnel est informé quant au fait qu'il lui est interdit d'utiliser les données personnelles d'une personne physique à des fins de prospection commerciale sans avoir préalablement obtenu son consentement.

La cession de tout ou partie d'un fichiers clients par une entreprise à une autre entreprise constitue une mise à disposition d'un traitement automatisé de données à caractère personnel au sens de l'article 2 de la loi du 6 janvier 1978.

Il convient donc d'agir en toute transparence quand l'opérateur de communications électroniques envisage de monétiser les données à caractère personnel qui concernent des individus dont il a recueilli les données.

Dans l'idéal, il faudra obtenir l'accord de l'utilisateur par le biais d'une case à cocher prévoyant que ce dernier est d'accord pour que ces données soient collectées à des fins de prospection commerciale.

UCOPIA WEB SERVICES :

La législation concernant l'utilisation de cookies et autres traceurs dans les supports de communications électroniques afin de proposer des contenus ciblés aux utilisateurs

Les utilisateurs de solutions informatiques permettant de proposer des contenus ciblés (publicités) aux internautes doivent savoir que la directive européenne dite « paquet télécom » les obligent à s'assurer que les internautes utilisant leurs plateformes donnent leur consentement préalablement à l'insertion de cookies et autres traceurs de ce type sur leurs machines.

Selon l'article 5(3) de la directive 2002/58/CE du 12 juillet 2002 modifié par l'adoption de la directive 2009/136/CE du 25 novembre 2009, il est, en effet, impératif d'obtenir, dans ce cas :

- « un consentement préalable de l'utilisateur avant le stockage d'informations sur l'équipement d'un utilisateur ou l'accès à des informations déjà stockées.

- sauf, si ces actions sont strictement nécessaires pour la délivrance d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur ».

L'article 32-II de la loi du 6 janvier 1978, modifié par l'ordonnance n°2011-1012 du 24 août 2011, lequel a transposé la directive 2009/136/CE, reprend cette exigence en précisant que :

« Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

- 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;

- 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 accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables 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 :

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

La réglementation envisagée précédemment concerne donc les cookies déposés et lus lors de la consultation d'un site internet, mais aussi lors de la lecture d'un courrier électronique et ce, quel soit le terminal utilisé tels qu'un ordinateur, un smartphone, une liseuse numérique, etc…

Le mot « cookie » utilisé est néanmoins à prendre avec un sens large.

Il recouvre, à titre d'exemple :

- Les cookies « HTTP »
- Les cookies « FLASH »
- Le résultat du calcul d'empreinte dans le cas du « fingerprinting » (calcul d'un identifiant unique de la machine basée sur des éléments de sa configuration à des fins de traçage).
- Les pixels invisibles ou « web bugs »
- tout autre identifiant généré par un logiciel ou un système d'exploitation

La CNIL a eu l'occasion de préciser que ces dispositions sont également valables pour des technologies apparentées aux cookies.

La liste de cookies précitée n'est donc pas exhaustive et concerne donc, de façon générale, l'ensemble des outils qui permettent de déterminer précisément ce qu'ont fait les utilisateurs à qui sont adressés des contenus ciblés.

Le terme « accord » visé par l'article 32-II de la loi du 6 janvier 1978 correspond au « consentement » défini à l'article 2 (h) de la directive 95/46/CE, c'est -à-dire à « toute manifestation de volonté, libre, spécifique et informée ».

La Commission Nationale Informatique et libertés (CNIL) considère que le consentement ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et n'est pas exposée à des conséquences négatives importantes dans l'hypothèse où elle refuse de donner son consentement.

La validité du consentement est donc liée à la qualité de l'information reçue.
Celle-ci doit être visible, mise en évidence et complète.

La CNIL recommande donc que l'information soit rédigée en des termes simples et compréhensibles pour tout utilisateur, et permette aux internautes d'être parfaitement informés des différentes finalités des Cookies déposés et lus.

Elle considère que l'utilisation d'une terminologie juridique ou technique trop complexe ne répondrait pas à l'exigence d'une information préalable.

Par exemple, si le cookie a pour finalité de « créer des profils d'utilisateurs afin d'adresser des publicités ciblées » , l'information devra reprendre l'ensemble de ces termes et non se limiter à indiquer "publicité".

La CNIL souligne, par ailleurs, 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.

Des systèmes adaptés doivent donc être mis en place pour recueillir le consentement selon des modalités pratiques qui permettent aux internautes de bénéficier de solutions conviviales et ergonomiques.

D'un point de vue pratique, avant de déposer ou lire un cookie, le responsable du traitement doit :

1. informer les internautes de la finalité des cookies
2. obtenir leur consentement
3. fournir aux internautes un moyen de les refuser

Dès lors, tant que la personne n'a pas donné son consentement, ces cookies ne peuvent être déposés ou lus sur son terminal.

Plusieurs options sont donc offertes :

Il est possible d'informer l'utilisateur par l'apparition d'un bandeau à l'écran :

a) Des finalités précises des cookies et de la technique de traçage utilisé, à savoir de « créer des profils d'utilisateurs afin d'adresser des publicités ciblées »

b) De la possibilité de s'opposer à ces cookies et de changer les paramètres en cliquant sur un lien « en savoir plus et paramétrer les cookies » présent dans le bandeau

c) Du fait que la poursuite de sa navigation vaut accord au dépôt de Cookies sur son terminal

Ce bandeau ne devra pas disparaître tant que l'internaute n'aura pas poursuivi sa navigation, en l'occurrence, tant qu'il n'aura pas cliqué sur un élément du site autre que le lien profond « en savoir plus et paramétrer les cookies ».

Le lien « en savoir plus et paramétrer les cookies » devra justement renvoyer sur une page dans laquelle seront présentées les solutions pour accepter ou refuser en tout ou partie les Cookies. Cette page devra être accessible sans dépôt de cookies et donc sans que cela occasionne une transmission d'informations.

La CNIL préconise également d'autres modalités de recueil du consentement.

Selon elle, les modalités de recueil de l'accord préalable peuvent également revêtir d'autres formes, telles que par exemple :

1. l'affichage d'une bannière décrivant les finalités des cookies utilisés, demandant explicitement à la personne si elle accepte le dépôt par familles de cookies , tout en lui précisant les moyens dont elle dispose pour retirer ultérieurement son consentement ;

2. une zone de demande de consentement en surimpression ;

3. une case à cocher lors de l'inscription à un service en ligne lui permettant d'accepter le dépôt de cookies par catégories de finalités ;

4. des boutons permettant d'activer les fonctionnalités d'un service déposant des cookies (par exemple, les plugins des réseaux sociaux).

La CNIL exige que les cookies ne puissent pas être conservés au-delà de 13 mois, délai qui ne saurait être prorogé lors des nouvelles visites.

UCOPIA WEB SERVICES :

UCOPIA s'engage, en tant que sous traitant aux données à caractère personnel du responsable du traitement qu'est l'opérateur de communications électroniques, à garantir la sécurité, la confidentialité et la disponibilité des données qu'il héberge pour le compte de ses clients.

UCOPIA s'engage notamment à :

- Conserver confidentielles toutes les données stockées sur ses serveurs et sur son infrastructure
- Ne pas prendre connaissance du contenu de ces données au delà de ce qui est nécessaire pour accomplir la mission qui lui été confiée par le Client et s'assurer que son personnel et ses commettants en feront de même
- Mettre en place des mesures de sécurité physique et logique des locaux et de son système d'informatique
- Assurer la sauvegarde des données et la continuité du service

Par ailleurs, conformément à l'article 68 qui dispose que :

« Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées ».

UCOPIA s'engage à ce que les données collectées par le responsable du traitement et hébergées par elle soient conservées sur des serveurs situés en France.

Par ailleurs, en tant que sous-traitant des données à caractère personnel, UCOPIA collaborera avec le responsable du traitement qui utilise ses produits afin qu'il puisse répondre aux droits d'accès, de modification, de suppression et d'opposition qu'il doit garantir à ses propres utilisateurs.

CONTACTUS@UCOPIA.COM
WWW.UCOPIA.COM

+33 1 40 92 73 90

201 AVENUE PIERRE BROSSOLETTE
92120 MONTROUGE - FRANCE