Les affaires de Privacy International, la Quadrature du net et al.

Royaume-Uni, Europe et Asie centrale

Affaire Résolue
Renforce la liberté d'expression

MODE D'EXPRESSION
Electronique / Communication sur internet

DATE DE LA DECISION
6 octobre 2020

NUMERO DE L'AFFAIRE
Affaire C-623/17, affaires C-511/18, C-512/18, C-520/18

ORGANE JUDICIAIRE
Cour de justice de l'Union européenne

TYPE DE DROIT
Droit civil, Droit constitutionnel

PRINCIPAUX THEMES:
Vie privée, protection et conservation des données

ISSUE :
Loi ou action annulée ou jugée inconstitutionnelle, avis consultatif/décision préliminaire

MOTS CLES :
Protection et conservation des données, Droit à la vie privée

L'examen comprend :

- L'analyse de l'affaire
- Le sens de la décision
- La perspective globale
- L'importance de l'affaire

ANALYSE DE L'AFFAIRE

Résumé et issue

La Cour de justice de l'Union européenne (CJUE), dans deux arrêts de Grande Chambre connexes, a statué que le droit de l'UE s'opposait à une législation nationale exigeant des fournisseurs de services de communications électroniques qu'ils procèdent à une transmission générale et indiscriminée des données relatives au trafic et des données de localisation aux agences de sécurité et de renseignement dans le but de protéger la sécurité nationale. Dans le cadre de demandes conjointes du Royaume-Uni, de la France et de la Belgique, la CJUE a cherché à déterminer la légalité d'une législation nationale qui prévoyait l'obligation pour les fournisseurs de services de communications électroniques de transmettre les données relatives au trafic et les données de localisation des utilisateurs à une autorité publique, ou de conserver ces données de manière générale ou indifférenciée pour des raisons de prévention de la criminalité et de sécurité nationale. La Cour a estimé qu'une telle obligation non seulement interférait avec la protection de la vie privée et des données à caractère personnel, mais était également incompatible avec le principe de la liberté d'expression prévu par l'article 11 de la Charte de l'Union européenne. La Cour a toutefois précisé que la conservation des données est justifiée en cas de menace grave pour la sécurité nationale ou l'ordre public, la nature de la mesure doit être « strictement » proportionnée à l'objectif poursuivi. En outre, la Cour a également clarifié l'étendue des pouvoirs conférés aux États membres par la directive sur la vie privée et les communications électroniques en ce qui concerne la conservation des données aux fins susmentionnées.

Les faits

Dans l'ensemble de l'UE, la conservation et l'accès aux données à caractère personnel dans le domaine des communications électroniques pour sauvegarder la sécurité nationale et lutter contre la criminalité ont été une pratique répandue parmi les agences de sécurité nationales. En particulier, la CJUE, dans l'affaire Tele2Sverige et Watson e.a. (C-203/15 et C-698/15, ci-après « Tele2 »), a estimé que les États membres ne peuvent pas imposer aux fournisseurs de services de communications électroniques une obligation de conservation générale et indifférenciée des données. Cela était gênant pour les États membres qui se voyaient privés d'un instrument de sauvegarde de la sécurité nationale. Sur cette base, quatre procédures distinctes ont été engagées contre des législations nationales au Royaume-Uni, en France et en Belgique concernant la légalité d'une obligation de conservation générale et indifférenciée

imposée aux fournisseurs de services de communications électroniques. Les détails de ces procédures sont donnés ci-dessous :

Affaire C-623/17 (Royaume Uni)

Le 5 juin 2015, une action a été introduite devant l'Investigatory Powers Tribunal (Royaume-Uni) par Privacy International, un groupe de défense basé au Royaume-Uni, concernant la légalité de la législation autorisant l'acquisition et l'utilisation de données de communication en masse par les agences de sécurité et de renseignement (à savoir le GCHQ, le MI5 et le MI6). Notamment, dans un jugement du 17 octobre 2016, les défendeurs avaient reconnu l'utilisation de données personnelles en vrac (telles que des données biographiques, de voyage, financières, commerciales et de communication) pour les analyser par recoupement et traitement automatisé, ainsi que pour les divulguer à d'autres personnes/autorités et partenaires étrangers. Ces données, acquises à partir des réseaux publics de communications électroniques, étaient utilisées par le GCHQ et le MI5 depuis 2001 et 2005 respectivement.

En analysant la régularité de ces pratiques, la juridiction de renvoi a estimé que les mesures d'acquisition et d'utilisation des données étaient conformes au droit national [paragraphe 6 de l'arrêt 1]. Notamment, les réseaux de communication électronique étaient tenus de fournir aux agences de sécurité et de renseignement les données collectées dans le cadre de leur activité économique, mais il n'en allait pas de même pour l'acquisition d'autres données obtenues par ces agences sans l'utilisation de pouvoirs contraignants. La Cour a donc jugé opportun de demander à la CJUE si (a) le régime juridique national relevait du champ d'application du droit communautaire et (b) si et de quelle manière les exigences de l'arrêt Tele2 s'appliquaient à ce régime.

Affaire C-511/18 (France)

Par des requêtes datées du 30 novembre 2015 et du 16 mars 2016, divers groupes de défense et organisations à but non lucratif ont déposé des demandes d'annulation de décrets devant le Conseil d'État qui imposaient aux opérateurs de communications électroniques et aux prestataires techniques de « mettre en œuvre sur leurs réseaux des traitements automatisés de données destinés [...] à détecter des liens susceptibles de constituer une menace terroriste », conformément à la loi française [paragraphe 25]. Les requérants soutenaient que les décrets violaient la Constitution française, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) et les directives 2000/31 et 2002/58 (concernant la protection des données à caractère personnel et de la vie privée).

Bien que la juridiction de renvoi ait conclu que l'obligation de conserver des données et l'accès des autorités administratives à ces données relevaient du champ d'application du droit de l'UE, elle a estimé que celui-ci ne s'étendait pas aux dispositions du droit national qui concernent spécifiquement les techniques de collecte de renseignements appliquées directement par l'État. Néanmoins, la Cour a jugé bon de suspendre la procédure et a renvoyé trois questions préjudicielles à la CJUE.

Affaire C-512/18 (France)

Par une requête du 15 septembre 2016, les associations de défense précitées ont formé un recours distinct contre une décision implicite de rejet de leur demande d'abrogation de textes législatifs qui porteraient atteinte à la vie privée en imposant une obligation de conservation générale et indifférenciée des données de communication à des fins judiciaires. La juridiction de renvoi a considéré que l'obligation de conservation et de rétention des données, telle qu'appliquée en l'espèce, ne relevait pas du droit de l'Union européenne, car son champ d'application était limité à la fourniture de services de communications électroniques accessibles au public sur les réseaux de communication publics dans l'Union européenne. Étant donné que le droit de l'UE ne prévoyait pas d'interdiction expresse de conserver de telles données, elle a également jugé bon de renvoyer l'affaire à la CJUE.

Affaire C-520/18 (Belgique)

Par des requêtes introduites en janvier 2017, la Cour constitutionnelle de Belgique a été saisie de plusieurs recours visant à l'annulation de la loi belge imposant la conservation des données. Les requérants soutenaient que la loi ne prévoyait pas de garanties de protection adéquates pour les données conservées et comportait un risque que des profils de personnalité puissent être établis et utilisés abusivement par les autorités compétentes. Ils ont affirmé que ces dispositions violaient la constitution belge, plusieurs dispositions de la CEDH, le PIDCP (Pacte international relatif aux droits civils et politiques) et le Traité sur l'Union européenne (TUE). Présentant des similitudes entre le droit national belge et le droit communautaire relatif à la conservation des données générées dans le cadre des réseaux de communication publics, la Cour constitutionnelle de Belgique a décidé de saisir la CJUE d'une question préjudicielle.

Par décisions du 25 septembre 2018 et du 9 juillet 2020, la Cour a joint les affaires C-511/18, C-512/18 et C-520/18. Elle a entendu séparément l'affaire C-623/17. Dans trois conclusions distinctes de l'avocat général Campos Sánchez-Bordona en date du 15 janvier 2020, l'avocat général a estimé que les activités menées par les autorités publiques des États membres pour des raisons de sécurité nationale et qui nécessitent la coopération de parties privées n'échappent pas au champ d'application de la directive 2002/58 sur la vie privée et les communications électroniques. Ainsi, lorsque les

fournisseurs de services de communications électroniques sont tenus par la loi de conserver des données et d'autoriser l'accès à ces données aux autorités publiques, les dispositions de la directive (en particulier le principe de confidentialité des communications prévu à l'article 5, paragraphe 1) sont applicables. Selon l'AG, les régimes nationaux doivent s'aligner sur les normes de la CJUE établies dans les affaires Tele2 et Digital Rights Ireland et autres, affaires C-293/12 et C-594/12 (« Digital Rights Ireland »), même dans les cas liés à la sécurité nationale.

Si les États membres sont autorisés à adopter des mesures législatives dans l'intérêt de la sécurité nationale, l'avocat général a également estimé que les limitations prévues à l'article 5, paragraphe 1, doivent être interprétées « strictement ». Il a recommandé une conservation et un accès limités aux données pour la prévention efficace de la criminalité et la sauvegarde de la sécurité nationale, mais a également ajouté que dans les cas justifiant une menace imminente ou un risque extraordinaire, la législation nationale était autorisée à imposer des obligations générales et étendues de conservation des données [paragraphe 16 des conclusions dans les affaires C 511/18 et C 512/18]. L'avocat général a indiqué que ces obligations qui conservent les données de manière générale ou indifférenciée en raison de menaces graves ou persistantes pour la sécurité nationale interféraient avec les droits fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne. Faisant valoir que la lutte contre le terrorisme n'était pas une question d'efficacité pratique mais d'efficacité juridique [paragraphe 5 des conclusions dans l'affaire C 623/17], il a estimé qu'une notification aux personnes concernées était une condition préalable nécessaire à la conservation des données, à moins que cela ne compromette l'action des autorités nationales.

L'avocat général a également déclaré que la collecte en temps réel de données relatives au trafic et de données de localisation n'était pas exclue par la directive, pour autant qu'elle soit effectuée dans le cadre des procédures établies et des garanties mentionnées ci-dessus. Cette obligation a été jugée applicable non seulement aux infractions graves, mais aussi aux infractions moins graves visées à l'article 23, paragraphe 1, du RGPD [paragraphe 9 des conclusions dans l'affaire C-520/18]. En ce qui concerne la question de savoir si la juridiction nationale peut maintenir les effets d'une loi nationale en cas d'incompatibilité avec le droit de l'UE, l'avocat général a estimé que cela était possible, mais uniquement si le maintien de ces effets était justifié et pour autant que cela soit strictement nécessaire pour corriger l'incompatibilité avec le droit de l'UE.

Aperçu de la décision

La Grande Chambre de la Cour a rendu une décision préjudicielle dans deux arrêts du 6 octobre 2020. La question principale posée à la Cour était le problème de l'application de la directive sur la vie privée et les communications électroniques aux activités liées à la sécurité nationale et à la lutte contre le terrorisme. La CJUE a formulé cinq questions à examiner :

La Grande Chambre de la Cour a rendu une décision préjudicielle dans deux arrêts du 6 octobre 2020. La question principale posée à la Cour était le problème de l'application de la directive sur la vie privée et les communications électroniques aux activités liées à la sécurité nationale et à la lutte contre le terrorisme. La CJUE a formulé cinq questions à examiner :

Une législation nationale permettant à une autorité étatique d'exiger des fournisseurs de services de communications électroniques qu'ils transmettent des données aux agences de sécurité et de renseignement pour la sécurité nationale relève-t-elle du champ d'application de la directive 2002/58 ?

L'article 15, paragraphe 1, de la directive 2002/58 doit-il être interprété en ce sens qu'il s'oppose à une législation nationale qui impose aux fournisseurs de services de communications électroniques, aux fins énoncées à l'article 15, paragraphe 1, une obligation de conservation générale et indifférenciée des données relatives au trafic et des données de localisation ?

L'article 15, paragraphe 1, de la directive 2002/58 doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale qui impose aux fournisseurs de services de communications électroniques de mettre en œuvre, sur leurs réseaux, des mesures permettant, d'une part, l'analyse automatisée et la collecte en temps réel de données relatives au trafic et à la localisation et, d'autre part, la collecte en temps réel de données techniques relatives à la localisation de l'équipement terminal utilisé, mais qui ne prévoit pas que les personnes concernées par ce traitement et cette collecte en soient informées ? [paragraphe 45]

Les dispositions de la directive 2000/31 doivent-elles être interprétées en ce sens qu'elles s'opposent à une réglementation nationale qui oblige les fournisseurs d'accès à des services de communication publique en ligne et les fournisseurs de services d'hébergement à conserver, de manière générale et indifférenciée, les données à caractère personnel relatives à ces services ? [paragraphe 49]

Une juridiction nationale peut-elle appliquer une disposition de droit national exigeant la conservation générale et indifférenciée de données relatives au trafic et à la localisation, en vue de poursuivre les objectifs de sauvegarde de la sécurité nationale/combattre la criminalité - bien que la législation soit incompatible avec l'article 15, paragraphe 1, de la directive 2002/58 ? [paragraphe 52]

L'article 5, paragraphe 1, de la directive 2002/58 sur la vie privée et les communications électroniques consacre le principe de la confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et prévoit l'interdiction pour les personnes autres que les utilisateurs de stocker, sans le consentement de ces derniers, ces communications et ces données. Toutefois, l'article

15, paragraphe 1, de la directive permet aux États membres d'introduire des exceptions au principe de l'article 5, paragraphe 1, lorsqu'une telle restriction est nécessaire pour sauvegarder la sécurité nationale.

En ce qui concerne la première question, la Cour a d'abord jugé que la directive 2002/58 sur la vie privée et les communications électroniques est applicable aux législations nationales exigeant la collecte et la conservation de données personnelles. Répondant négativement à l'argument des défendeurs selon lequel les activités des agences de sécurité et de renseignement sont des fonctions essentielles de l'État et relèvent donc de la seule responsabilité des États membres, en dehors du champ d'application de la directive, la CJUE a estimé que le champ d'application de la directive s'étend non seulement aux mesures législatives exigeant la collecte et la conservation de données, mais aussi aux mesures législatives exigeant que les fournisseurs de services accordent l'accès à ces données. En effet, ces mesures législatives requièrent nécessairement le traitement de données par les fournisseurs de communications électroniques et ne peuvent donc pas être considérées comme des activités caractéristiques des États. La Cour a cité le RGPD pour noter que la divulgation de données à caractère personnel par transmission (comme le stockage ou toute autre forme de mise à disposition de données) constituait un « traitement » (le RGPD désigne la notion de « traitement de données à caractère personnel » comme toute opération sur des données à caractère personnel qui constitue une collecte, un stockage, une utilisation, une consultation, une divulgation par transmission, une diffusion ou toute autre forme de mise à disposition de données). (paragraphe 15 de l'affaire C-623/17).

En revanche, la CJUE a déclaré que la seule circonstance où la protection des données des personnes n'est pas couverte par le droit de l'UE est celle où les États membres mettent directement en œuvre des mesures sans imposer d'obligations de traitement aux fournisseurs de services de communication électronique.

Après s'être prononcée sur l'applicabilité de la directive 2002/58 dans les affaires jointes examinées, la Cour s'est penchée sur l'impact du droit à la sécurité consacré par l'article 15, paragraphe 1, de la directive 2002/58 et la Charte des droits fondamentaux de l'UE (article 6 - Droit à la liberté et à la sécurité). Plus précisément, les juridictions de renvoi ne savaient pas si la conservation des données prévue par les législations nationales interférait avec les articles 7 (respect de la vie privée et familiale) et 8 (protection des données à caractère personnel) de la Charte. En confirmant l'arrêt Tele2 et Watson et autres, la CJUE a jugé que la directive 2002/58 ne permet pas de transformer en règle l'exception à l'obligation de principe d'assurer la confidentialité des communications électroniques et des données y afférentes et à l'interdiction de conservation de ces données (prévue à l'article 5, paragraphe 1). Par conséquent, la Cour a conclu que la directive n'autorise pas les États membres à adopter des mesures législatives qui restreignent la portée des droits aux fins de la sécurité nationale, à moins qu'une telle

mesure ne soit conforme aux principes généraux du droit de l'UE, tels que le principe de proportionnalité et les droits fondamentaux garantis par la Charte. [paragraphe 35]

Il est important de noter que la Cour a reconnu que le fait d'imposer aux fournisseurs de services de communications électroniques, par le biais de législations nationales, l'obligation de conserver les données relatives au trafic, non seulement interfère avec la protection de la vie privée et des données à caractère personnel, mais est également incompatible avec le principe de la liberté d'expression prévu à l'article 11 de la Charte de l'Union européenne. Non seulement la Cour a rappelé l'importance de la vie privée et de la liberté d'expression dans l'interprétation de l'article 11 de la directive, mais elle a également estimé que la conservation des données constituait en soi une dérogation au principe de confidentialité de l'article 5, paragraphe 1, puisqu'elle interdit à toute personne autre que l'utilisateur de stocker ces données. La Cour n'a pas jugé pertinent de faire une distinction entre les données sensibles et non sensibles ou le fait que les données conservées aient été utilisées ultérieurement ou non.

Le risque de profilage revêt une importance particulière pour la Cour : la possibilité d'utiliser les données relatives au trafic et les données de localisation pour obtenir des informations sur des aspects de la vie privée (tels que les opinions politiques, l'orientation sexuelle, les croyances religieuses, l'état de santé, les relations sociales, etc.) et de tirer des conclusions précises sur la vie privée des personnes dont les données ont été conservées constituait une menace directe pour le droit à la vie privée. Par conséquent, d'une part, la conservation des données à des fins policières constituait en soi une violation du droit au respect des communications et, d'autre part, la simple conservation de données en quantités importantes par les fournisseurs de communications électroniques comportait un risque d'abus et d'accès illicite.

Dans ce contexte, la Cour a répondu à la deuxième question par l'affirmative, en considérant que la directive européenne s'oppose à une législation nationale exigeant des fournisseurs de services de communications électroniques qu'ils procèdent à la transmission générale et indiscriminée de données relatives au trafic et de données de localisation aux agences de sécurité et de renseignement aux fins de sauvegarder la sécurité nationale. En outre, elle a également déclaré qu'une telle pratique, même à titre préventif, est exclue par le droit de l'Union, en particulier pour les obligations qui conservent les données de manière générale ou indifférenciée et lorsqu'il n'existe aucun lien entre le comportement des personnes dont les données sont affectées et l'objectif poursuivi par la législation en cause.
La Cour a toutefois précisé que lorsqu'une telle conservation est justifiée en cas de menace grave pour la sécurité nationale ou publique, la nature de la mesure doit être « strictement » proportionnée à l'objectif poursuivi. Un objectif de mesure générale ne peut être poursuivi que s'il est concilié avec les droits fondamentaux (interprétation de l'article 15(1)). Plus important encore, la Cour a précisé qu'une

décision imposant une telle ordonnance doit être soumise à un contrôle effectif, soit par la Cour, soit par un organe administratif indépendant doté d'un pouvoir contraignant. La Cour a également appelé à l'adoption de règles claires et précises au niveau national régissant la portée et l'application de la conservation des données afin de se prémunir contre les risques d'abus.

Une distinction a toutefois été faite par la Cour pour la conservation des données relatives à l'identité civile des utilisateurs de systèmes de communication électronique. Dans la mesure où il n'est pas possible de connaître la date, l'heure, la durée et les destinataires dans de tels cas, il n'est pas non plus possible de dresser un profil de la vie privée. Pour une telle conservation ciblée sur la base d'éléments objectifs ou non discriminatoires (selon des catégories de personnes concernées ou un critère géographique), une mesure législative imposant aux fournisseurs de communications électroniques de conserver ces données est autorisée même en l'absence de lien entre l'ensemble des utilisateurs de systèmes de communications électroniques et les objectifs poursuivis [paragraphe 42]. De même, la conservation des adresses IP attribuées à la source de la communication est également autorisée si elle est limitée à ce qui est strictement nécessaire. Enfin, lorsque la conservation des données au-delà des délais légaux de conservation des données est nécessaire et que des infractions ont déjà été constatées ou que leur existence est raisonnablement soupçonnée, une mesure législative n'est pas exclue par la directive.

Sur la troisième question, la juridiction de renvoi avait observé que les techniques automatisées de collecte de renseignements et la collecte en temps réel de données techniques n'étaient légales que dans l'intention de prévenir le terrorisme et non autrement. À titre préliminaire, la CJUE a noté que les données faisant l'objet d'une analyse automatisée à des fins de prévention du terrorisme constituent des « données à caractère personnel » au sens du RGPD, car les informations peuvent toujours être attribuées à une personne spécifique. Sur cette base, la Cour a conclu que cette analyse automatisée des données relatives au trafic et à la localisation était contraire au principe de confidentialité de la directive 2002/58 ainsi qu'aux droits fondamentaux de la Charte de l'UE, et qu'elle était susceptible d'avoir un effet dissuasif sur l'exercice de la liberté d'expression.

Même dans ce cas, la doctrine de la proportionnalité « stricte » était applicable, si une ingérence était jugée nécessaire en raison d'une menace grave pour la sécurité nationale. Les conditions à remplir pour satisfaire le test de proportionnalité étaient les suivantes : (a) la menace pour la sécurité nationale doit être réelle et actuelle ou prévisible et (b) la durée de cette rétention est limitée à ce qui est strictement nécessaire. Des modèles ou des critères préétablis aux fins d'une analyse automatisée (tels que l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale, ou des informations sur la santé ou la vie sexuelle d'une personne) dans le but de prévenir le terrorisme, ne peuvent donc pas être basés sur des données sensibles isolées [paragraphe 47]. La Cour

a appliqué un raisonnement similaire pour la collecte en temps réel de données personnelles. La collecte de telles données n'est pas exclue par la directive uniquement si elle est limitée aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles soient impliquées dans une activité terroriste et si elle est soumise à un contrôle préalable par un tribunal ou une autorité administrative indépendante contraignante.

En ce qui concerne la quatrième question, la Cour a interprété l'article 23, paragraphe 1, du RGPD (qui prévoit des restrictions au traitement des données à caractère personnel) ainsi que la Charte comme s'opposant à une législation nationale exigeant des fournisseurs d'accès à des services de communication en ligne et des fournisseurs de services d'hébergement qu'ils conservent, de manière générale et sans distinction, les données à caractère personnel relatives à ces services. La Cour a appliqué les conclusions tirées dans le cadre des questions susmentionnées à l'article 23 du RGPD également.

Enfin, la CJUE a tranché la dernière question, relative au maintien des effets dans le temps d'une législation nationale jugée incompatible avec le droit de l'UE. Elle a jugé que les juridictions nationales ne peuvent pas appliquer une disposition du droit national les habilitant à limiter les effets dans le temps d'une déclaration d'illégalité qu'elles sont tenues de faire en vertu de ce droit. Cette décision se fonde sur le principe de primauté de l'UE, qui établit la prééminence du droit de l'UE sur le droit des États membres. Toutefois, la CJUE a également estimé qu'il appartient au droit national de déterminer les règles relatives à l'admissibilité et à l'évaluation des informations obtenues par la conservation de données en violation du droit de l'UE, dans le cadre de procédures pénales à l'encontre de personnes suspectes [paragraphe 53]. Les juridictions pénales nationales sont néanmoins tenues de ne pas tenir compte des informations ou des preuves obtenues au moyen d'une conservation générale ou indifférenciée des données relatives au trafic et des données de localisation en violation du droit communautaire - lorsque les personnes soupçonnées d'avoir commis des infractions pénales ne sont pas en mesure de commenter efficacement ces informations (en vertu du principe d'effectivité). La CJUE a donc également répondu par la négative à la dernière question.

SENS DE LA DECISION

Issue : Renforce la liberté d'expression

La surveillance de masse a un effet dissuasif sur la liberté d'expression. La décision de la CJUE dans cette affaire constitue une avancée significative dans les efforts de protection des droits fondamentaux à la liberté de parole et d'expression dans l'Union européenne. Dans les quatre affaires, la Cour a utilisé

le contrôle "strict" comme norme pour l'action législative, ce qui exige que les États membres exercent la collecte et la conservation des données pour servir uniquement des intérêts impérieux de l'État, sans lien avec la répression des idées. L'affaire réaffirme que l'échange d'idées et le libre exercice de l'expression sont des valeurs positives et importantes - non seulement pour ceux qui exercent leurs droits, mais pour toute la société.

PERSPECTIVE GLOBALE

Sommaire des références

Lois internationales et/ou régionales pertinentes

- CJUE, Tele2 Sverige AB c. Post- och telestyrelsen, Secretary of State for the Home Department c. Watson, affaires jointes C 203/15 et C 698/15 (2016).
- CEDH, Commission c. Hongrie (Transparence des associations) (2020), C-78/18.
- CEDH, K.U. c. Finlande (2008), requête n° 2872/02.
- CEDH, Von Hannover c. Allemagne (2004), req. 59320/00.
- CEDH, M.C. c. Bulgarie (2004), Req. n° 39272/98.
- CEDH, Osman c. Royaume-Uni (1998), Req. n° 87/1997/871/1083.
- CEDH, El-Masri c. " L'ex-République yougoslave de Macédoine " (2012), Req. n° 39630/09.
- CEDH, Medvedye et autres c. France (2010), Req. n° 3394/03.
- CEDH, Ladent c. Pologne (2008), Req. n° 11036/03.
- CJUE, Commission c. Hongrie (Droits d'usufruit sur les terres agricoles) (2019), C-235/17, EU:C:2019:432.
- CJUE, Rayonna prokuratura Lom (2019), C-467/18, EU:C:2019:765.
- CJUE, Digital Rights (2014), C-293/12 et C-594/12, EU:C:2014:238.
- CJUE, Volker und Markus Schecke et Eifert (2010), C-92/09 et C-93/09, EU:C:2010:662.
- CJUE, Satakunnan Markkinapörssi et Satamedia (2008), C-73/07, EU:C:2008:727.
- CJUE, Ministerio Fiscal (2018), C-207/16, EU:C:2018:788.
- CJUE, Facebook Ireland et Schrems (2020), C-311/18, EU:C:2020:55.
- CEDH, Ben Faiza c. France (2018), Req. n° 31446/12.
- CJUE, SNB-REACT (2018), C-521/17, EU:C:2018:639.
- CJUE, Mc Fadden (2016), C-484/14, EU:C:2016:689.
- CJUE, SABAM (2012), C-360/10, EU:C:2012:85.

- CJUE, Scarlet Extended (2011), C-70/10, EU:C:2011:771.
- CJUE, Österreichischer Rundfunk et autres (2003), C-465/00, C-138/01 et C-139/01, EU:C:2003:294.
- CJUE, Communications Skype (2019), C-142/18, EU:C:2019:460.
- CJUE, Popławski (2019), C-573/17,EU:C:2019:530.
- CJUE, Melki et Abdeli (2010), C-188/10 et C-189/10,EU:C:2010:363.
- CJUE, A. K. et autres (Indépendance de la chambre disciplinaire de la Cour suprême) (2019), C-585/18, C-624/18 et C-625/18, EU:C:2019:982.
- CJUE, Flaminio Costa c. E.N.E.L. (1964), affaire 6/64, EU:C:1964:66.
- CJUE, Inter-Environnement Wallonie et Bond BeterLeefmilieu Vlaanderen (2019), C-411/17, EU:C:2019:622.
- CJUE, A et autres (Éoliennes à Aalter et Nevele) (2020), C-24/19, EU:C:2020:503.
- CJUE, Nelson et autres (2020), C-581/10 et C-629/10, EU:C:2012:657.

IMPORTANCE DE L'AFFAIRE

La décision établit un précédent influent ou persuasif au sein de sa juridiction.

La décision (y compris les opinions concordantes ou dissidentes) établit un précédent influent ou persuasif en dehors de sa juridiction.

DOCUMENTS OFFICIELS DE L'AFFAIRE

- Jugement (anglais)
- AG Opinion on C-511/18 - 512/18 15 Jan 2020
- AG Opinion on C-520/18 15 Jan 2020
- AG Opinion on C-623/17

Rapports, analyses et articles de presse :

- **La Cour suprême de l'UE empêche les États de collecter les données des utilisateurs à des fins de surveillance**
  https://www.ft.com/content/71cc07fb-58ff-404d-868c-5dd0e8a97e20
- **Dans son arrêt, la plus haute juridiction de l'UE estime que les régimes britannique, français et belge de surveillance de masse doivent respecter la vie privée, même dans le cadre de la sécurité nationale**

https://privacyinternational.org/press-release/4205/press-release-ruling-eus-highest-court-finds-uk-french-and-belgian-mass

- **Q&R : La plus haute juridiction de l'UE juge que les régimes de surveillance de masse britannique, français et belge doivent respecter la vie privée**
  https://privacyinternational.org/long-read/4206/qa-eus-top-court-rules-uk-french-and-belgian-mass-surveillance-regimes-must-respect