Aperçu scientifique CS-2022-DR-030 – PUBLIC 3 février 2023

La conservation et l'exploitation de données à caractère personnel par les opérateurs du secteur des communications électroniques

Pour citer le document : R. El Herfi, « La conservation et l'exploitation de données à caractère personnel par les opérateurs du secteur des communications électroniques », Luxembourg, Cellule scientifique de la Chambre des Députés, 3 février 2023.

Résumé

- La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques consacre **le principe de la confidentialité des données relatives au trafic et des données de localisation générées par l'utilisation de services de communications électroniques**.

- Cette directive crée des obligations pour les opérateurs, comme l'effacement ou l'anonymisation de telles données lorsqu'elles ne sont plus nécessaires à la transmission d'une communication ou encore le recueil du consentement des utilisateurs lorsque leurs données peuvent être traitées à des fins commerciales.

- **Cette protection peut toutefois être limitée**. L'article 15, paragraphe 1 de la directive 2002/58/CE permet aux États membres d'adopter des mesures législatives restrictives de cette protection, qui prévoient, par exemple, la conservation des données par les opérateurs.

- La limitation doit toutefois constituer « **une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques (…)** ». La mesure de limitation, adoptée dans le respect des principes généraux du droit de l'Union européenne, doit être d'une durée limitée et justifiée par les motifs d'intérêt général mentionnés ci-dessus.

- Dans un contexte de lutte plus accrue contre le terrorisme et la criminalité, les États membres ont été amenés à adopter de telles réglementations. Certaines de ces législations ont donné lieu à une jurisprudence récente et fournie de la Cour de justice de l'Union européenne précisant les exigences auxquelles elles doivent répondre, particulièrement l'exigence de proportionnalité.

- La Cour affirme **le principe de l'interdiction de la conservation généralisée indifférenciée et de l'exploitation des données de connexion**. Elle apporte des

nuances à ce principe, en précisant aux autorités nationales qu'afin que leurs réglementations soient conformes à **l'exigence de proportionnalité** de l'article 15, paragraphe 1 de la directive, elles doivent **mettre en relation le niveau de gravité de l'ingérence avec le niveau de gravité de la menace qui la justifie**.

- Cette analyse a ainsi conduit la Cour à admettre, dans des conditions strictement définies, qu'une législation puisse imposer aux opérateurs de communications électroniques une conservation généralisée et indifférenciée des données de connexion lorsqu'elle poursuit des finalités de sécurité publique.

- Ces arrêts rendus par la Cour de justice impliquent une **lecture renouvelée de l'article 15, paragraphe 1 de la directive 2002/58/CE** et exigent, en conséquence, des États membres d'adapter leurs législations afin de se conformer avec les exigences clarifiées. C'est dans ce contexte que s'inscrit le « Projet de loi relative à la rétention des données à caractère personnel et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État » présenté le 25 janvier 2023 par Madame la Ministre de la Justice.

Table des matières

La protection des données à caractère personnel a connu une évolution parallèle au développement des nouvelles technologies et de l'environnement numérique. Les données de connexion ou métadonnées, objet de la directive 2002/58/CE, nécessitent une protection particulière puisqu'une simple connexion implique plusieurs intermédiaires comme les fournisseurs de communication, les fournisseurs d'hébergement ou encore les fournisseurs d'accès à internet qui, potentiellement, peuvent détenir un important nombre de données.

L'importance de ces données les érige à la fois **en objet de protection à des fins de garantie de la vie privée mais aussi en objet d'exploitation à des fins sécuritaires**, puisqu'elles peuvent servir de preuves dans le cadre de diverses procédures pénales. Ainsi, les États ont été amenés à adopter des législations, impliquant de plus en plus les opérateurs du secteur des communications électroniques pour conserver et parfois exploiter de telles données, si bien que ces opérateurs privés sont perçus comme de « nouveaux agents en charge de l'application de la loi »[1].

Le présent aperçu tente, à partir du cadre réglementaire européen, de l'analyse des législations nationales et de la jurisprudence de la Cour de justice, de mettre en lumière les éléments d'un équilibre **entre deux exigences potentiellement en conflit : la protection des données à caractère personnel et l'objectif légitime de sûreté de l'État.**

1. Le cadre légal relatif au traitement des données de connexion par les opérateurs du secteur des communications électroniques

1.1 Le cadre européen de protection des données de connexion

Le droit à la protection des données à caractère personnel est un droit fondamental[2], consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne[3] mais également par l'article 16 du Traité sur le fonctionnement de l'Union européenne[4].

La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données pose les premiers jalons de la protection des données personnelles en Europe. Assurant une protection « omnibus », elle s'applique tant au secteur privé qu'au secteur public. Elle définit les notions de « données à caractère personnel », de « traitement » de celles-ci, de « responsable de traitement », pose les principes directeurs relatifs au traitement licite des données à caractère personnel[5] et prévoit l'établissement d'autorités indépendantes de contrôle dans les États membres. Le cadre

[1] S. Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors", *Computer Law & Security Review*, 2021, Volume. 43, 17 p.
[2] À noter que l'article 31 de la Constitution luxembourgeoise (issu de la récente révision constitutionnelle) prévoit que:
« Toute personne a droit à l'autodétermination informationnelle et à la protection des données à caractère personnel la concernant. Ces données ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi. »
[3] L'article 8, paragraphes 1 et 2, de la Charte énonce que :
« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. ».
On notera aussi que la protection des données à caractère personnel est aussi très liée à la protection de la vie privée, garantie par l'article 7 de la Charte.
[4] Selon l'article 16, paragraphe 1, TFUE :
« Toute personne a droit à la protection des données à caractère personnel la concernant. »
[5] C. Castets-Renard, « La protection des données personnelles dans les relations internes à l'Union européenne », *Répertoire Dalloz*, Octobre 2018 (mis à jour en novembre 2022), points 18-39.

juridique général qu'offre cette directive a été réformé à l'issue de l'adoption, en 2016, du règlement général sur la protection des données (dit « RGPD »)[6].

À l'aune de ce cadre juridique général, la directive 2002/58/CE représente une *lex specialis* : elle reprend les principes directeurs de la directive 95/46/CE pour les adapter au secteur des communications électroniques. Particulièrement, cette directive :

- Consacre le **principe de confidentialité** des communications effectuées au moyen des réseaux publics de communication[7] ;
- Assure la protection des données personnelles des **personnes privées comme des personnes morales**[8] ;
- Précise la notion de **« données de localisation »**, en les définissant comme « toutes données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public »[9] ;
- Crée l'obligation **d'effacer ou de rendre anonymes les données relatives au trafic ou à la localisation** lorsqu'elles ne sont plus nécessaires à la transmission d'une communication ou à la facturation[10] ;
- Encadre les communications non sollicitées ou **spamming**, en créant une obligation de recueillir, préalablement à tout profilage marketing, le consentement de l'utilisateur[11] ;
- Crée un droit d'information et un droit de refus des **cookies** (témoins de connexion), autrement dit leur utilisation n'est autorisée qu'à condition que des informations claires et précises soient fournies aux utilisateurs sur la finalité des cookies ou de dispositifs similaires[12].

En raison de l'évolution constante des technologies dans ce secteur, la directive a connu plusieurs réformes, dans le but de maintenir un niveau élevé de protection des données à caractère personnel et de la vie privée des utilisateurs des services. La directive 2002/58 a notamment été modifiée par la directive 2006/24/CE[13].

Invalidée par la Cour de justice en 2014[14], cette directive créait une obligation incombant aux opérateurs de services de communication électroniques de conserver pendant une certaine durée, tout type de données de connexion et d'en permettre l'accès à des autorités nationales, sans encadrer cet accès par quelconque finalité, limitation ou garantie contre les abus.

En conséquence de l'invalidation de la directive 2006/24/CE, la Commission a soumis, en 2017, une proposition de règlement dit « **règlement e-Privacy** »[15] qui demeure encore en débat. Visant à harmoniser les législations nationales limitant la confidentialité des communications électroniques, la proposition prévoit d'encadrer de manière plus stricte l'utilisation des données de connexion au prisme des exigences dressées par la Cour de justice.

---

[6] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. Ce règlement est applicable depuis le 25 mai 2018.
[7] Article 5, paragraphe 1 de la directive 2002/58/CE.
[8] La directive 95/46/CE ne protège que les données des personnes privées.
[9] Article 2 de la directive 2002/58/CE.
[10] Article 6, paragraphe 1 de la directive 2002/58/CE.
[11] Article 13, paragraphe 1 de la directive 2002/58/CE.
[12] Article 5, paragraphe 3 de la directive 2002/58/CE.
[13] 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.
[14] Arrêt du 8 avril 2014 (grande chambre), Digital Rights Ireland et Seitlinger e.a. (affaires jointes C-293/12 et C-594/12, EU:C:2014:238).
[15] Proposition de règlement européen du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM/2017/010 final du 10 janvier 2017.

Les données de connexion en tant que « données à caractère personnel »

- L'article 4, paragraphe 1 du RGPD définit les « données à caractère personnel » comme « **toute information se rapportant à une personne physique identifiée ou identifiable (…); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale**».

- **La notion de « données de connexion » ou de « métadonnées »**, définie en détail à l'article 2 de la directive 2002/58/CE, **correspond à une large catégorie de données de trafic et de localisation générées lors de communications téléphoniques ou informatiques**. Ces données entrent dans la définition ci-dessus mais elles peuvent aussi entrer dans la définition des **« données sensibles »** telles que définies par l'article 9 du RGPD puisqu'elles peuvent renseigner sur les convictions politiques, religieuses, philosophiques, sur l'orientation sexuelle ou l'état de santé.

- **Exemples de métadonnées** :
  - ⇨ Les adresses IP des terminaux des utilisateurs d'un fournisseur d'accès à internet (voir arrêt du 19 octobre 2016, Breyer (C-582/14, EU:C:2016:779)
  - ⇨ Les données de localisation
  - ⇨ Les données de facturation (nom, prénom, adresse…)
  - ⇨ Les adresses URL des sites visités
  - ⇨ Les dates et les heures de connexion
  - ⇨ Les numéros de téléphone des appels entrants et sortants
  - ⇨ Les messages envoyés et reçus (sms notamment)
  - ⇨ La date, l'heure, la durée des appels
  - ⇨ La géolocalisation de l'appelant

1.2 Les possibles limitations du principe de confidentialité des données de connexion

Le fonctionnement de Union européenne se fonde sur un système de répartition des compétences entre l'Union et ses États membres, si bien que certains domaines d'action demeurent de la seule responsabilité de ces derniers. Il en est ainsi des « des fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale (…). », comme le prévoit l'article 4, paragraphe 2 du Traité sur l'Union européenne (TUE).

L'article 1er, paragraphe 3, la directive 2002/58/CE se fait l'écho de l'article 4, paragraphe 2 TUE, en ce qu'il prévoit que la directive « ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne [...] et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal. ».

Les États membres sont-ils alors exemptés de leurs obligations au titre de la protection des données personnelles et de la confidentialité des communications lorsqu'ils adoptent des réglementations concernant la sécurité publique, la défense ou le droit

pénal ? Le risque ici serait qu'une interprétation extensive de la notion de sécurité nationale se fasse au détriment d'une interprétation restrictive de la notion de donnée personnelle[16].

Certains États membres ont, en effet, tenté de remettre en cause l'applicabilité de la directive 2002/58/CE à chaque fois qu'il s'agissait d'interpréter la conformité de leurs législations à la lumière de cette dernière[17]. La Cour de justice s'appuie néanmoins sur la dérogation prévue par l'article 15, paragraphe 1 de la directive pour confirmer que celle-ci reste bel et bien applicable.

L'article 15, paragraphe 1, de la directive 2002/58/CE prévoit que « [l]es États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

Pour la Cour de justice, l'existence même de cette dérogation et de l'encadrement qu'elle prévoit, justifient que les législations nationales limitatives du principe de confidentialité des communications tombent dans le champ d'application de la directive. C'est précisément du fait que « les autorités nationales s'appuient sur des opérateurs privés pour collecter les données de connexion qui fait basculer la situation dans le champ d'application du droit de l'Union »[18]. L'article 1er, paragraphe 3 de la directive couvrirait ainsi l'hypothèse où les autorités nationales opèrent elles-mêmes la collecte des données de connexion.

[16] Cela était particulièrement le cas de la législation britannique RIPA (Regulation of Investigating Powers Act) adoptée au cours de l'année 2000 et réglementant les pouvoirs des institutions publiques qui mènent des activités de surveillance, des écoutes téléphoniques notamment pour des raisons de sécurité nationale. *Voy.* A cet égard : A. Taleb-Karlsson, « Protection des données personnelles et sécurité nationale au Royaume-Uni : quelles leçons tirer du droit anglo-saxon ? », in D. Beauregard-Berthier, A. Taleb-Karlsson (dir.), *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?* Bruylant, 2017, pp.227-248.

[17] Affaires Tele2 Sverige (affaires jointes C-203/15 et C-698/15) ou Privacy International (C-623/17) et La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18).

[18] R. Tinière, Cour de justice, gde ch., 6 octobre 2020, La Quadrature du Net e.a., aff. jtes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, in F. Picod (dir.), *Jurisprudence de la CJUE 2020. Décisions et commentaires*, Bruylant, 2020, p. 132.

Quant à **l'encadrement** de la dérogation prévue par l'article 15, paragraphe 1er de la directive, il implique une mise en balance entre d'une part, l'objectif d'intérêt général (*sauvegarde de la sécurité nationale, de la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*) et, d'autre part, les droits en cause (*confidentialité des données de connexion, effacement ou anonymisation des données de trafic, de localisation, non présentation de l'identification de la ligne appelante ou de la ligne connectée*). Cette mise en balance se fait en **mesurant d'abord la gravité de l'ingérence que crée la législation en cause et en évaluant, ensuite, si l'importance de l'objectif poursuivi serait en relation avec cette gravité**. La jurisprudence de la Cour de justice offre à cet égard une « esquisse d'un tableau de concordance entre les atteintes et les risques pour la sécurité »[19].

PRINCIPE : ARTICLES 5, 6, 8 ET 9 DE LA DIRECTIVE 2002/58/CE

Droit à la protection des données de connexion

- Confidentialité des communications électroniques
- Effacement ou anonymisation des données de trafic et de localisation
- Non présentation de l'identification de la ligne appelante ou de la ligne connectée

DÉROGATION : ARTICLE 15, PARAGRAPHE 1 DE LA DIRECTIVE 2002/58/CE

Possibilité pour un État d'adopter une mesure de conservation des données
Conditions

- **Finalité de la mesure** : objectif légitime de sauvegarde de la sécurité nationale, de la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.
- **Nécessité et adéquation de la mesure :** aucune autre mesure ne permet de réaliser adéquatement l'objectif poursuivi et la mesure offre des garanties suffisantes d'efficacité.
- **Proportionnalité de la mesure :** la gravité de la limitation est en correspondance avec la gravité de l'objectif légitime poursuivi.

[19] A. Deroudille, « L'exploitation généralisée et indifférenciée des données de connexion en question », *Revue de l'Union européenne*, 2022, p.332.

2. Les exigences jurisprudentielles encadrant les mesures de conservation des données de connexion

2.1 Affirmation du principe d'interdiction d'une conservation généralisée et indifférenciée et d'une exploitation des données de connexion

L'arrêt ***Digital Rights Ireland*** porte les prémisses du principe d'interdiction d'une conservation générale et indifférenciée des données à caractère personnel par les opérateurs du secteur des communications électroniques. Par cet arrêt, la Cour de justice, saisie par la High Court irlandaise et par le Verfassungsgerichtshof autrichien en appréciation de la validité de la directive 2006/24/CE, était amenée à apprécier, notamment au regard de l'article 8 de la Charte, la conformité de l'obligation, prévue par ladite directive, incombant aux opérateurs de services de communications électroniques de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications ainsi que d'en permettre l'accès à des autorités nationales compétentes.

La Cour invalide la directive au motif que :

- Les dispositions de la directive comportent **une ingérence particulièrement grave** dans le respect des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte ;

- Cette ingérence, bien que susceptible d'être justifiée par la poursuite d'un objectif d'intérêt général tel que la lutte contre la criminalité organisée, **excède les limites qu'impose le respect du principe de proportionnalité** (absence d'un encadrement suffisant susceptible de garantir que l'ingérence soit limitée au strict nécessaire).

Dans la foulée de l'invalidation de la directive 2006/24/CE, l'arrêt *Tele2 Sverige et Watson* apporte un premier éclaircissement sur l'interprétation de la marge d'appréciation laissée aux États membres lors de l'adoption de réglementations nationales visant la conservation des données de connexion. Saisie au sujet de la règlementation suédoise[20] et la règlementation britannique[21], la Cour énonce le principe de l'interdiction d'une conservation généralisée et indifférenciée des données de connexion. Pour la Cour, l'article 15, paragraphe 1 de la directive 2002/58/CE permet aux États membres de déroger notamment au principe de confidentialité des données et en tant que disposition dérogatoire, il doit être soumis à une **interprétation stricte**.

La Cour précise :

- Que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière de la Charte, s'oppose à une réglementation nationale prévoyant, **à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des**

[20] La directive 2006/24/CE avait fait l'objet d'une transposition dans le droit suédois par l'introduction de la loi (2003 :389) sur les communications électroniques et par le règlement (2003 :396) sur communications électroniques. La loi suédoise prévoyait la même obligation de conservation des données de connexion que celle prévue par la directive et couvrait également diverses autres données liées aux appels téléphoniques (notamment liées aux appels n'ayant pas abouti et la localisation de l'émetteur). L'ordre fait aux opérateurs privés de conserver puis de transmettre ces appels n'était soumis à aucun contrôle préalable de légalité et l'accès aux données n'était pas strictement limité à des personnes ou des autorités identifiées (bien que la loi précisât que les personnes ayant eu connaissance de ces données étaient soumises au secret professionnel). La durée de conservation était limitée à six mois, au-delà desquels les données devaient faire l'objet d'un effacement.

[21] Il s'agit de la Data retention Act 2014 (« DRIPA ») ainsi que de la Regulation of Investigatory Act 2014 (RIPA). En vertu de la DRIPA, le secrétaire d'État britannique peut demander à un opérateur du secteur des communications électroniques de conserver des données, pour une période maximale de douze mois lorsqu'il s'agit de données pertinentes, au sens de la RIPA qui énumère les motifs d'intérêt public, tels que la sécurité nationale notamment. Si la conservation des données ne comprend pas le contenu des communications, elle concerne néanmoins tout type de données de connexion. Les avis de conservation émis par le secrétaire d'État sont confidentiels et ne sont pas soumis à un contrôle ou une autorisation judiciaire préalable. La divulgation des données aux autorités publiques doit être nécessaire et proportionnelle au regard des motifs d'intérêts public énumérés par la RIPA.

données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

- Que cet article doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et à la localisation, permettant l'accès des autorités nationales compétentes aux données conservées
- ⇨ **sans limiter cet accès aux seules fins de lutte contre la criminalité grave**,
- ⇨ sans le soumettre à un **contrôle préalable** par une juridiction ou une autorité administrative indépendante,
- ⇨ et sans exiger que les données en cause soient conservées **sur le territoire de l'Union**.

Elle précise toutefois que cette dérogation ne s'oppose pas à une réglementation nationale qui permet, **à titre préventif, à des fins de lutte contre la criminalité grave**, **la conservation ciblée** de données, à condition qu'elle soit **limitée au strict nécessaire** en ce qui concerne les catégories de données, les personnes concernées, les moyens de communication et la durée de conservation. Cela implique :

- Que la règlementation nationale prévoie **des règles claires et précises pour protéger efficacement les données contre les abus (circonstances et conditions d'adoption des décisions de conservation) ;**

- Que la règlementation nationale définisse **les éléments objectifs établissant un rapport entre les données à conserver et l'objectif poursuivi** (données susceptibles de révéler un lien avec des actes de criminalité grave, données contribuant à la lutte contre la criminalité grave ou à la prévention de risques graves pour la sécurité publique).

2.2 Les nuances admises par l'examen de la proportionnalité entre la gravité de l'ingérence et l'importance de l'objectif général poursuivi

APPORT ESSENTIEL DE LA JURISPRUDENCE DEPUIS L'ARRÊT « QUADRATURE DU NET ET FDN » (2020)

- Cette jurisprudence opère une **concordance entre la gravité de l'ingérence et l'importance du risque encouru.**
- Cela implique une **« échelle »[22] des objectifs poursuivis et donc une « échelle » du type de conservation.**
- La marge d'intervention des États **varie aussi selon la nature des données** (leur nécessité pour réaliser l'objectif légitime poursuivi, leur sensibilité).

Échelle de gravité des objectifs (par ordre décroissant) :

- Prévention de menaces graves (réelles et actuelles ou prévisibles) contre la sécurité publique
- Lutte contre la criminalité grave
- Sauvegarde de la sécurité nationale
- Prévention, recherche, détection et poursuite d'infractions pénales (lutte contre la criminalité en général)

Échelle de sensibilité des données (par ordre décroissant) :

- Données de trafic et localisation
- Adresses IP : ne révèlent aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication
- Identités civiles des utilisateurs de moyens de communication : ne permettent pas de connaître la date, l'heure, la durée, les destinataires, les lieux ou fréquences des communications (hypothèse d'une législation qui subordonne l'achat d'une carte SIM à la vérification préalable et l'enregistrement de l'identité de l'utilisation)

La Cour de justice poursuit son analyse du principe d'interdiction d'une conservation générale et indifférenciée des données à caractère personnel par les opérateurs du secteur des communications électroniques en affinant sa jurisprudence[23], spécifiquement en ce qui concerne l'encadrement de la marge laissée aux États membres pour apprécier la proportionnalité de leurs réglementations dérogatoires prises en vertu de l'article 15, paragraphe 1 de la directive 2002/58/CE. Autrement dit, **cette jurisprudence détermine les différentes obligations générales à la charge des États dont le respect conditionne la proportionnalité de ces règlementations dérogatoires**.

En effet, cette jurisprudence admet **une conservation des données de connexion plus ou moins ciblée ou plus ou moins générale et indifférenciée**, lorsque les réglementations nationales poursuivent **les objectifs de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique**. L'étendue des obligations des États **varie selon la nature des données en cause**.

[22] En ce sens, *voy*. : J. Sirinelli, « La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite », *Revue trimestrielle de droit européen*, 2021, n° 2, pp. 313-330

[23] Arrêt du 2 octobre 2018 (grande chambre), Ministerio Fiscal (C-207/16, ECLI:EU:C:2018:788) ; arrêts du 6 octobre 2020 (grande chambre), Privacy International (C-623/17, EU:C:2020:790) et La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) ; arrêt du 2 mars 2021 (grande chambre), Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152) ;arrêt du 5 avril 2022 (grande chambre), Commissioner of the Garda Síochána (C-140/20, EU:C:2022:258) ; arrêt du 20 septembre 2022 (grande chambre), SpaceNet et Telekom Deutschland, (affaires jointes C-793/19 et C-794/19, EU:C:2022:702) et arrêt du 20 septembre 2022 (grande chambre), VD et SR, (affaires jointes C-339/20 et C-397/20, EU :C :2022 :703).

LES EXIGENCES JURISPRUDENTIELLES ENCADRANT LA PROPORTIONNALITÉ DES LÉGISLATIONS NATIONALES RELATIVES À LA CONSERVATION OU L'EXPLOITATION DES DONNÉES DE CONNEXION

Interdiction d'une conservation généralisée et indifférenciée et d'une exploitation des métadonnées à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales.

Nuances et précision du principe :

Admission de certaines réglementations nationales prescrivant la conservation de métadonnées, lorsque celles-ci poursuivent les finalités suivantes :

- **Sauvegarde de la sécurité nationale,**
- **Lutte contre la criminalité grave**
- **Prévention des menaces graves contre la sécurité publique**

Conditions :

- La gravité de l'ingérence doit être en rapport avec l'importance de l'objectif général poursuivi par la réglementation.
- Les circonstances et les conditions d'adoption des décisions de conservation sont claires et précises (précision éventuellement des catégories de données, de personnes concernées, délimitation d'une période temporelle/zone géographique)
- Durée de conservation des données limitée dans le temps bien que pouvant être renouvelée
- Conservation soumise à des garanties strictes : contrôle effectif par une juridiction ou une autorité administrative indépendante de la demande de conservation ou de son renouvellement

S'agissant des règlementations portant sur l'exploitation des données de connexion (traitement automatisé des données de connexion) :

- Hypothèse du traitement automatisé en temps réel des données de trafic et de localisation seulement en cas de menace grave pour la sécurité nationale qui s'avère réelle, actuelle ou prévisible
- Soumission aux mêmes conditions que les réglementations relatives à la conservation des données de connexion (voir ci-dessus)
- Les modèles et les critères préétablis sur lesquels se fondent le traitement des données doivent être spécifiques et fiables (critères permettant une identification sans discrimination liée à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou politique, l'appartenance syndicale, l'état de santé ou la vie sexuelle)
- Tout résultat positif doit être soumis à un réexamen individuel et non automatisé
- Les modèles et critères préétablis de traitement doivent être régulièrement réexaminés afin d'assurer leur fiabilité continue et leur actualisation.

Sont ainsi admis :

- La conservation préventive généralisée et indifférenciée des données de trafic et de localisation à des fins de sauvegarde de la sécurité publique : ***en cas de menace grave pour la sécurité nationale qui s'avère réelle, actuelle ou prévisible***
- La conservation ciblée des données de trafic et de localisation à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales : ciblage notamment en fonction des personnes concernées ou de zones géographiques spécifiées
- La conservation préventive généralisée et indifférenciée des adresses IP aux fins de la lutte contre la criminalité et la sauvegarde de la sécurité publique
- La conservation préventive généralisée et indifférenciée des données relatives à l'identité

Bibliographie :

Jurisprudence

- Arrêt du 8 avril 2014 (grande chambre), Digital Rights Ireland et Seitlinger e.a. (affaires jointes C-293/12 et C-594/12, EU:C:2014:238).
- Arrêt du 19 octobre 2016, Breyer (C-582/14, EU:C:2016:779).
- Arrêt du 21 décembre 2016 (grande chambre), Tele2 Sverige (affaires jointes C-203/15 et C-698/15, EU:C:2016:970).
- Arrêt du 2 octobre 2018 (grande chambre), Ministerio Fiscal (C-207/16, ECLI:EU:C:2018:788).
- Arrêts du 6 octobre 2020 (grande chambre), Privacy International (C-623/17, EU:C:2020:790) et La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791).
- Arrêt du 2 mars 2021 (grande chambre), Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152).
- Arrêt du 5 avril 2022 (grande chambre), Commissioner of the Garda Síochána (C-140/20, EU:C:2022:258).
- Arrêt du 20 septembre 2022 (grande chambre), SpaceNet et Telekom Deutschland, (affaires jointes C-793/19 et C-794/19, EU:C:2022:702).
- Arrêt du 20 septembre 2022 (grande chambre), VD et SR, (affaires jointes C-339/20 et C-397/20, EU :C :2022 :703).

Voir aussi :

- Cour de justice de l'Union européenne, Direction de la recherche et documentation, Fiche thématique sur la protection des données à caractère personnel, Novembre 2021, 70 p.

Monographies et articles

- D. Beauregard-Berthier, A. Taleb-Karlsson (dir.), *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?* Bruylant, 2017, 279 p.
- C. Castets-Renard, « La protection des données personnelles dans les relations internes à l'Union européenne », *Répertoire Dalloz*, Octobre 2018 (mis à jour en novembre 2022).
- R. Perray, « Fasc. 1230 : Données à caractère personnel – Introduction et champ d'application de la réglementation relative à la protection des données personnelles », *JurisClasseur Europe Traité*, 8 avril 2019 (mis à jour le 4 septembre 2022).

- B. Bertrand, « Les enjeux de la surveillance numérique », *Revue trimestrielle de droit européen*, 2021, n° 1, pp. 175-180.
- B. Bertrand, « Les précisions sur l'interprétation et l'application du régime de l'e-privacy », *Revue trimestrielle de droit européen*, 2022, n° 3, pp. 481-484.
- X. Bréchot, « Clap de fin pour la conservation généralisée des données de connexion en Europe ? », *Revue de l'Union européenne*, 2017 n° 606 pp.178-187.
- C. Castets-Renard, Cour de justice, gde ch., 6 octobre 2020, La Quadrature du Net e.a., aff. jtes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, in F. Picod (dir.), *Jurisprudence de la CJUE 2020. Décisions et commentaires*, Bruylant, 2020, pp. 1091-1100.
- C. Copain- Héritier, « Le cadre européen de la protection des données : entre forces et faiblesses intrinsèques », *Revue de l'Union européenne*, 2022, n° 646 pp.163-171.

- A. Denis-Fatôme, « Données de connexion et lutte contre la criminalité », *Communication – Commerce électronique*, n°7-8, comm. 52
- A. Deroudille, « L'exploitation généralisée et indifférenciée des données de connexion en question », *Revue de l'Union européenne*, 2022, pp.332
- J. Sirinelli, « La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite », *Revue trimestrielle de droit européen*, 2021, n° 2, pp. 313-330
- R. Tinière, Cour de justice, gde ch., 6 octobre 2020, La Quadrature du Net e.a., aff. jtes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, in F. Picod (dir.), *Jurisprudence de la CJUE 2020. Décisions et commentaires*, Bruylant, 2020, pp. 130-139.
- S. Tosza, "Internet service providers as law enforcers and adjudicators. A public role of private actors", *Computer Law & Security Review*, 2021, Volume. 43, 17 p.
- X. Tracol, "The joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States", *Computer law & security review*, 2023, Volume 48, 14 p.
- X. Tracol, "Two jugments of the European Court of Justice in the four cases of Privacy International, La Quadrature du Net and Others, French Data and Ordre des Barreaux francophone et germanophone and Others: The Grand Chamber is trying hard to square the circle of date retention", *Computer law & security review*, 2021, Volume 41, 13 p.

Auteur : Racha El Herfi

Requérant : M. Sven Clement

Luxembourg, le 3 février 2023