Kristian Turkalj[1]

LES ENJEUX DE LA RÉGLEMENTATION SUR LA CONSERVATION DES DONNÉES DE COMMUNICATIONS ÉLECTRONIQUES À LA LUMIÈRE DE LA JURISPRUDENCE DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

UDK: 347.9 (4)
DOI: 10.31141/zrpfs.2020.57.135.53
Izvorni znanstveni rad
Primljeno: 1. prosinca 2019.

Les questions de législation induites par la conservation des données issues des communications électroniques constituent depuis quelques années déjà un défi pour l'Union européenne. En effet, il convient de trouver un équilibre entre les mesures à prendre pour garantir la sécurité, notamment face au terrorisme et au crime organisé, tout en garantissant la protection de la vie privée et la protection du respect des droits fondamentaux des individus. Après les attaques terroristes commises aux Etats-Unis et en Europe lors de la précédente décennie, il est apparu nécessaire d'introduire des obligations concernant la collecte et la conservation des données de communications électroniques afin de lutter efficacement contre le terrorisme et les formes graves de criminalité. Les mesures prises au niveau de l'Union visent à fixer un cadre législatif à la conservation des données. Il est incontestable que la conservation de ces données constitue un outil utile et efficace à des fins de prévention et de détection d'infractions graves ainsi que pour les enquêtes et les poursuites en la matière. Cependant, il est vrai aussi qu'il existe un risque d'atteinte aux garanties relatives aux droits et libertés des individus notamment les droits à la confidentialité et à la liberté d'expression garantis par la Charte des droits fondamentaux.

La Cour de justice de l'Union européenne a mis en évidence, dans les jugements concernant Digital Rights et Tele2, une violation des droits fondamentaux dans les dispositions législatives relatives à la conservation des données prises au niveau national et européen. Ce texte s'intéresse à la portée des arrêts en question sur la législation nationale et analyse les principales normes relatives à la protection des droits de l'homme en matière de conservation des données, pratique relevée par la Cour européenne dans les décisions qu'elle a rendues. Suite à l'arrêt de la Cour européenne de justice, les États membres de l'UE, y compris la République de Croatie, ont été confrontés à un défi de taille pour améliorer le cadre juridique de la conservation des données. A cet égard, une analyse approfondie du cadre juridique national s'avère nécessaire tout comme un réexamen de certaines décisions afin de se conformer pleinement aux exigences et aux critères fixés par la Cour européenne.

Mots-clés: *Acquis communautaire, Conservation des données, Cour de justice de l'Union européenne, Directive sur la conservation des données, Données relatives au trafic, Confidentialité des communications électroniques, Sécurité, Terrorisme, Vie privée, Protection des données à caractère personnel*

[1] Kristian Turkalj, Secrétaire d'état au Ministère de la Justice, RC

I. INTRODUCTION

La nécessité d'introduire des obligations portant sur la collecte et la conservation des données de communications électroniques pour une protection plus efficace de la sécurité publique et nationale dans le cadre de la lutte contre le terrorisme, le crime organisé et les infractions pénales graves dans les États membres de l'Union européenne, s'est manifestée dans la dernière décennie du siècle dernier[2]. Dès cette époque, les autorités judiciaires ont souligné le fait que le déroulement des poursuites était sérieusement entravé par le manque de données issues des communications électroniques.

Plusieurs évènements ont eu un impact décisif dans le domaine de la régulation normative de la conservation des données relatives aux communications électroniques dans l'Union européenne : les actes terroristes survenus aux États-Unis, à Madrid et à Londres[3]. Ces attaques ont particulièrement touchées l'opinion publique et ont contribuées à donner l'avantage aux questions de sécurité par rapport à la protection des droits de l'homme. Dans cet esprit et prenant acte du problème de l'importance des données, le législateur européen a pris une série de mesures concrètes se traduisant notamment par l'établissement d'obligations pour les fournisseurs de services de communications électroniques et les réseaux publics de télécommunication de stocker les données de ses utilisateurs pendant une période donnée et de veiller à ce que les données conservées puissent être mises à la disposition des autorités compétentes afin de garantir la défense et la sécurité nationale et permettre le bon déroulement des détections, des enquêtes et des poursuites en la matière. Dans ce contexte, un certain nombre d'instruments législatifs sont adoptés en 2002 et 2006 afin de réguler le régime de conservation des données – la Directive relative à la vie privée et aux communications électroniques[4] et la Directive sur la conservation des données[5].

Cependant, dans son arrêt *Digital rights*[6] d'avril 2014, la Cour de justice de l'Union européenne a invalidé la Directive sur la conservation des données, seul instrument de régulation en la matière au niveau européen, au motif que l'obligation générale de conservation des données constitue une ingérence caractérisée dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel.

---

[2] Dragičević D. et Gumzej N. (2014.) Obvezno zadržavanje podataka i privatnost, Zbornik Pravnog fakulteta u Zagrebu, Vol. 64 No.1 2014.; pp. 39-79.

[3] Concernant les conséquences des attentats terroristes sur la politique de l'Union en matière de lutte contre le terrorisme voir: Turkalj, K., Pravni i institucionalni okvir Europske unije za suzbijanje terorizma, doktorska disertacija, Zagreb, 2011., pp. 82-101.

[4] Directive 2002/58/CE du Parlement européen et du Conseil, JO L 201 du 31/07/2002, 32002L0058/FR 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

[5] Directive 2006/24/CE 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

[6] Voir l'arrêt de la Cour (grande chambre) du 8 avril 2014 (Affaires jointes C-293/12 et C-594/12); Recueil de jurisprudence

Dans l'arrêt *Tele2* de décembre 2016[7], la Cour va un peu plus loin encore en indiquant que le droit de l'Union s'oppose à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données. Ainsi, la Cour indique que le droit de l'Union n'est pas compatible avec l'obligation générale de conservation des données aux fournisseurs imposée par les régimes nationaux des États membres.

La portée de la jurisprudence est considérable dans la mesure où il n'existe plus d'harmonisation européenne sur la conservation et l'accès des données et de protection uniforme des droits des citoyens de l'Union. Les États membres se trouvent privés de cadre européen définissant des lignes directrices claires pour les régimes nationaux concernant la conservation des données amenant à des situations hétérogènes dans les différents États membres de l'Union. Dans certains États membres, les cours constitutionnelles ont annulé les réglementations nationales tandis que d'autres ont de leur propre initiative conservé les cadres nationaux existants ou ont créé de nouveaux cadres permettant la conservation des données. Ces cadres sont, sans l'existence de règles communes adoptées par tous les États membres, hétérogènes et incohérents entre eux.

Les questions principales résident donc dans la recherche d'une solution adéquate au problème de la conservation des données de communications électroniques qui concilie les exigences en matière de protection des droits fondamentaux et les critères fixés par la Cour de justice de l'Union européenne, d'une part, et les besoins des autorités compétentes dans la détection, la prévention et la poursuite des infractions terroristes et du crime organisé d'autre part. Ainsi, il s'agit de construire un cadre législatif conforme en prenant en compte le fait que le droit de l'Union 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 et l'accès des autorités nationales à ces données soumis à un contrôle préalable d'un organisme indépendant avec des garanties supplémentaires concernant les données personnelles conservées.

II. LA PROTECTION DE L'INTÉRÊT PUBLIC ET DE L'INTÉRÊT PRIVÉ IMPLIQUANT DES DROITS AUX CARACTÈRES OPPOSÉS

La conservation des données des communications électroniques est un outil très précieux pour les autorités en charge de la protection de l'ordre public et de la sécurité nationale. Cela permet la détection, la prévention, l'investigation et la poursuite du terrorisme et de la criminalité grave. Par conséquent, l'usage en est

[7] Voir l'arrêt de la Cour (grande chambre) du 21 décembre 2016 (Affaires jointes C-203/15 et C-698/15) ; Recueil de jurisprudence

préventif comme répressif. Mais, par ailleurs, la conservation des données empiète sur les droits et libertés fondamentaux des citoyens qui sont garantis par des instruments juridiques internationaux. En ce qui concerne les États membres de l'Union Européenne, il s'agit notamment de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et de la Charte des droits fondamentaux de l'Union européenne (ci-après: Charte).

La Charte affirme les droits qui résultent principalement des traditions constitutionnelles et des obligations internationales communes aux États membres, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, des chartes sociales adoptées par l'Union et par le Conseil de l'Europe ainsi que par la jurisprudence de la Cour de justice de l'Union européenne. La Charte constitue le droit primaire de l'UE et présente la même obligation juridique pour les États membres que les traités fondateurs de l'UE. En ce qui concerne la conservation des données, il est important de souligner que la Charte précise que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications (art. 7), à la protection des données à caractère personnel la concernant (art. 8), à la liberté d'expression qui comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières (art. 11). Or ces droits peuvent être sérieusement atteint par une mesure de conservation des données car elle rend possible une intrusion dans la vie privée des individus et entraine la crainte d'un suivi qui peut encourager à limiter la communication et l'expression par le biais des communications électroniques.

Bien que ces droits soient garantis et protégés, ils ne sont pas pour autant illimités et absolus. D'après l'article 8, paragraphe 2, de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales et suivant l'interprétation de la Cour européenne des droits de l'homme, il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à l'ordre public, à la santé économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. Ainsi, l'État peut prendre des mesures limitant les droits fondamentaux des individus pour protéger certains intérêts si l'ingérence reste conforme à la loi et que celle-ci est suffisamment précise et claire pour permettre aux individus de l'appréhender. La limitation doit se faire dans un cadre démocratique et les objectifs visés se doivent d'être légitimes. La réalisation de la mesure doit résulter d'un besoin social urgent et doit être prise en adéquation avec l'objectif visé dans une démarche cherchant constamment à éviter de s'ingérer dans les droits fondamentaux.

Il n'est généralement pas contesté que le droit de l'Union européenne autorise des dérogations du principe de protection absolue des droits fondamentaux lorsqu'il est nécessaire de préserver d'autres intérêts légitimes. La question est plutôt de savoir si ces mesures restreignant les droits fondamentaux sont indispensables et,

le cas échéant, proportionnées par rapport à l'objectif légitime visé. En effet, il convient de garder à l'esprit que la Charte, en plus des droits susmentionnés, garantit à tous les citoyens le droit à la liberté et à la sûreté (art. 6). Bien qu'il existe une certaine vigilance sur l'importance de protéger ces intérêts, notamment dans les domaines de la liberté et de la sécurité pour les citoyens européens, dans le contexte actuel de lutte contre le terrorisme et la criminalité, il apparait que la protection du droit du citoyen au respect de la vie privée et familiale, de son domicile et de ses communications et de ses droits à la protection des données à caractère personnel et à la liberté d'expression devient un impératif de plus en plus important dans un contexte où règne la nécessité de sécuriser l'espace européen. La question cruciale pour les législateurs au niveau national et européen est de savoir où tracer la ligne de démarcation entre ces droits qui s'opposent. Les droits de l'homme doivent-ils s'imposer face aux questions de sécurité nationale et de lutte contre le terrorisme et le crime organisé? Si aucun de ces droits ne prévaut sur les autres, peuvent-ils être complémentaires? En effet, ne prenons nous pas le risque, dans l'objectif de protéger la liberté et les droits de l'homme, de dégrader paradoxalement cette même liberté et ces mêmes droits? Toutes ces questions ouvrent le débat sur les valeurs qui doivent prévaloir dans une société démocratique et, en fin de compte, sur le type de société dans laquelle nous voulons vivre.

En ce sens, le défi est de trouver un équilibre entre les objectifs de l'Union européenne en matière de sécurité et de lutte contre les formes modernes de terrorisme et de criminalité organisée d'une part, et le droit au respect de la vie privée d'autre part, en particulier la protection des données personnelles des individus qui doit rester un droit fondamental de toute société qui se veut démocratique et pluraliste car elle est partie intégrante des valeurs sur lesquelles l'Union est fondée. Ainsi, dans ses arrêts rendus concernant la conservation des données, l'UE a établi des lignes directrices grâce auxquelles on doit pouvoir établir une proportionnalité dans la limitation des droits fondamentaux pour la protection d'objectifs légitimes.

Par conséquent et compte tenu des considérations de la Cour qui insistent sur la nécessité de respecter pleinement les droits fondamentaux que garantit la Charte, nous considérons que les solutions proposées, qui introduiraient un principe de proportionnalité dans la législation nationale sur la conservation des données, doivent faire l'objet d'une attention toute particulière. En effet, ces mesures, qui se veulent nécessaires, appropriées et proportionnées, doivent se faire conformément aux droits fondamentaux énoncés par la Charte. Il faut notamment éviter les situations où, conformément à l'arrêt de la Cour de l'UE, on défendrait les droits individuels des articles 7 et 8 de la Charte, mais cela au détriment d'autres droits mentionnés dans celle-ci. Par exemple, selon l'arrêt *Tele2*, la limitation des droits fondamentaux est envisageable lorsque les autorités nationales, sur la base d'éléments objectifs, identifient une ou plusieurs zones géographiques où existe un risque accru de préparation ou d'exécution d'actes de terrorisme ou de grande criminalité. Cependant, cela questionne quant à l'atteinte potentielle des droits fondamentaux d'autres personnes de la même zone géographique dont les données pourraient être à priori collectées alors même qu'elles ne sont impliquées à aucun moment dans des

actes répréhensibles. Pourtant, la limitation à une zone géographique spécifique ou à un moyen de communication spécifique pourrait fortement nuire à la prévention des infractions criminelles graves car les auteurs potentiels peuvent gagner en mobilité et facilement échapper aux systèmes de surveillance. Par ailleurs, il faut garder à l'esprit que les actes terroristes actuels sont rarement préparés sur le territoire de leur exécution, où sur un territoire bien défini qui serait aisément détectable par les autorités compétentes.

Compte tenu de tout cela, il sera nécessaire à l'avenir de trouver des solutions satisfaisantes pour assurer le plein respect des droits fondamentaux des citoyens garantis par la Charte des droits fondamentaux de l'Union européenne tout en fournissant aux autorités les outils indispensables pour mener à bien des enquêtes ciblées. Il faut garder à l'esprit qu'une limitation trop importante de l'obligation générale de conservation des données pourrait exclure de la conservation des données importantes et ainsi avoir des conséquences négatives sur le système de lutte contre le terrorisme et les infractions pénales graves.

III. L'IMPORTANCE DE LA CONSERVATION DES DONNÉES POUR L'ACTIVITÉ DE L'AUTORITÉ CHARGÉE DES POURSUITES

L'importance de conserver les données de communications électroniques pour lutter contre toutes les formes contemporaines de terrorisme et d'infraction pénale grave est incontestable. Les données conservées jouent un rôle crucial dans la poursuite des infractions pénales mais aussi dans les actions préventives visant à détecter les réseaux criminels et terroristes susceptibles de passer à l'acte. En outre, la conservation des données peut jouer un rôle important en dehors du cadre de la lutte contre le terrorisme et le crime organisé, comme par exemple dans le cas de recherche de personnes disparues où les dernières données de communication peuvent jouer un rôle clé dans l'enquête. De plus, ces données peuvent être de toute première importance lorsqu'il s'agit de fournir un alibi pour prouver l'innocence d'une personne.

Les données conservées fournissent aux autorités chargées des poursuites un moyen supplémentaire d'investigation grâce auquel il est possible de prévenir ou d'éclaircir les infractions pénales graves. En effet, à la différence des mesures de surveillance ciblées, une telle mesure permet aux autorités d'accéder au passé de l'individu concerné. Les mesures de surveillance ciblées se concentrent sur les personnes qui ont eu potentiellement un lien, même faible ou indirect, avec des activités criminelles graves. Ces mesures ciblées permettent aux organismes compétents en la matière d'accéder aux données relatives aux communications mais aussi au contenu de ces communications. Les données accessibles se limitent cependant à la communication seulement après que la personne concernée a été identifiée. L'obligation générale de conservation de données se rapporte elle

à l'ensemble des communications de l'ensemble des utilisateurs sans que ceux-ci soient nécessairement suspectés d'infraction pénale grave. Les autorités compétentes ont ainsi accès à l'historique des communications d'individus encore non identifiés comme étant liés à des activités criminelles. Autrement dit, l'utilité de la conservation générale des données dans la lutte contre les infractions graves réside dans la possibilité encadrée d'avoir accès au passé sur la base de la consultation de l'historique des communications d'individus avant même qu'ils ne soient suspectés[8].

La Commission européenne a présenté un rapport en 2011 qui traite de la mise en œuvre de la Directive sur la conservation des données dans les États membres dans lequel il est souligné l'importance de la conservation des données en tant que moyen précieux, voire indispensable, dans la prévention et la lutte contre la criminalité, la protection des victimes et la disculpation d'individus innocents[9]. Sur la base de données statistiques et d'exemples illustrés fournis par les États membres sur le rapport de corrélation entre les données conservées et le nombre de condamnations et d'acquittements, c'est-à-dire le non-lieu à statuer de procédures et la prévention de la criminalité, il est possible de tirer un certain nombre de conclusions sur le rôle et la valeur de la conservation des données à des fins pénales. Par exemple, la police autrichienne a utilisé les données conservées dans 92% des enquêtes menées sur une période de seulement 3 mois quand la police allemande utilisait les données conservées comme seul et unique moyen de mener l'enquête dans 44,5% des cas, Au Royaume-Uni, les données conservées se sont avérées être d'une importance cruciale dans quasiment toutes les enquêtes qui ont mené à des condamnations.

Au Royaume-Uni, en 2012, une étude a révélé que 84% des données conservées qui ont permis de mener avec succès les poursuites pénales dataient de moins de 6 mois. Dans la plupart des cas, les auteurs d'infractions pénales n'étaient pas connus de la police auparavant. Les données des communications électroniques ont été alors d'une importance décisive pour recueillir les preuves nécessaires et assurer ainsi le bon déroulement de l'enquête. Sans conservation des données, la majorité des auteurs n'auraient jamais été découverts et poursuivis[10].

La pratique montre qu'un grand nombre de cas n'aurait pas pu être traités en raison du manque de données conservées, c'est-à-dire que ces données représentent une valeur ajoutée significative dans la réussite de la procédure pénale. En ce qui concerne les poursuites pénales, selon les dispositions législatives actuelles, les données de communication électroniques concernant le suspect ou l'accusé sont disponibles de telle sorte que ces données sont conservées de manière rétroactive dans le cadre des données globales détenues contre un nombre illimité de personnes pour les besoins de l'enquête et des poursuites, et en sont extraites par la suite au

[8] Conclusions de l'avocat général Henry Saugmandsgaard Øe dans les affaires jointes BAE C-203/15 Tele2 Sverige AB / Post-och telestyrelsen et C-698/15 Secrétaire d'Etat à Home Department / Tom Watson et al. du 19 juillet 2016; p. 25

[9] Rapport de la Commission au Conseil et au Parlement européen ; Rapport d'évaluation concernant la directive sur la conservation des données (Directive 2006/24/EC); Bruxelles, 18.4.2011 COM(2011) 225 final; pp. 23-25

[10] Age of communications data requested (2012 ACPO SPOC survey)

cas par cas. Pour les autorités chargées des poursuites, il est difficile de détecter les auteurs potentiels d'infractions pénales de sorte que seules les données les concernant sont conservées. Ces données sont extrêmement importantes pour mener l'enquête et permettre d'identifier tous les acteurs impliqués dans l'exécution d'une infraction grave et tout particulièrement dans les cas de poursuites d'infractions terroristes. En effet, il est de la plus haute importance de déterminer le cercle des personnes qui ont communiqué avec l'auteur avant ou pendant l'attaque afin de pouvoir retrouver l'ensemble du réseau terroriste. Seules les données conservées peuvent fournir des informations précises sur le suspect et son mode opératoire et permettent d'identifier avec qui elle était en contact intense lors de la préparation de l'acte. Pour cette raison, les autorités compétentes doivent conserver les données pour pouvoir enquêter de manière efficace notamment lorsque seules les données permettent de démarrer l'enquête.

IV. CADRE JURIDIQUE DE LA CONSERVATION DES DONNÉES DANS L'UNION

En 1996, sur le modèle de l'expérience américaine, l'Union a entamé d'intenses discussions et réflexions sur l'introduction d'un régime de conservation des données électroniques aux fins d'enquêtes et de poursuite d'infractions pénales[11]. Les dispositions à l'époque (Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications) contraignaient les fournisseurs de services à conserver les données relatives au trafic exclusivement à des fins de facturation pour les abonnés qui sont traités aux fins de la transmission d'une communication ou de coûts de facturations et de recouvrement, et concernait les abonnés ou les utilisateurs de service pour une durée de moins de 3 mois. Ce cadre n'étant pas satisfaisant pour les autorités chargées des poursuites, le législateur de l'Union a décidé de mettre en place le cadre de conservation des données tel que nous le connaissons aujourd'hui.

L'introduction des nouvelles technologies numériques dans le réseau public de communication a amené de nouvelles exigences relatives à la protection des données personnelles et de la vie privée des utilisateurs et rendu nécessaire l'adoption de lois et de réglementations afin de protéger les droits et libertés fondamentaux des citoyens de l'Union. Ainsi, la Directive sur la vie privée et les communications électroniques a été adoptée en 2002. Elle vise à garantir dans l'Union un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, face au traitement des données à caractère personnel dans le secteur des communications électroniques mais a aussi pour objectif d'assurer la libre circulation de ces données dans l'Union

[11] Drewry, L. (2016) Crimes without culprits: Why the European union needs data retention, and how it can be balanced with the right to privacy. Wisconsin International Law Journal, p. 732.

européenne. Outre l'obligation faite aux États membres d'assurer la confidentialité des communications, la Directive prévoit une exception importante dans l'article 15, paragraphe 1. Conformément à la disposition susmentionnée, les Etats membres peuvent adopter des mesures législatives limitant la portée de certains droits et de certaines obligations individuelles de la Directive lorsqu'une telle restriction constitue une mesure nécessaire appropriée et proportionnée dans le cadre d'une société démocratique et qu'elle vise à protéger la sécurité nationale (défense nationale et publique) dans l'objectif de prévenir les infractions graves et de se donner les moyens nécessaires pour l'investigation et les poursuites. En ce sens, les États membres peuvent adopter des mesures permettant la conservation de données dans la mesure où elles s'exercent sur une période déterminée et qu'elles sont justifiées par la réglementation[12].

Cependant, la situation sécuritaire en Europe se dégradant très nettement, notamment du fait des attaques terroristes visant les grandes métropoles européennes[13], il est apparu nécessaire de mettre en place un outil adapté encadrant de manière claire et précise la conservation des données de communications électroniques[14]. Le Conseil „Justice et Affaires intérieures" de l'Union européenne a adopté le 19 décembre 2002 des conclusions qui soulignent l'importance des données relatives à l'utilisation des communications électroniques pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment lorsqu'il s'agit de criminalité organisée. Dans sa déclaration sur la lutte contre le terrorisme publiée le 25 mars 2004, le Conseil européen charge le Conseil de l'UE de renforcer la réglementation des données relatives au trafic de communications pour les fournisseurs de services, tandis que la Déclaration du 13 juillet 2005 du conseil de l'UE condamnant les attaques terroristes réaffirmait la nécessité d'adopter le plus rapidement possible des mesures communes concernant la conservation des données de télécommunication[15].

Ces éléments que nous venons de mentionner en lien avec la volonté d'harmoniser les dispositions relatives à la conservation des données de communication électroniques compte tenu des différences importantes entre les dispositions nationales conformément à la Directive précédente, à savoir la 2002/58/CE, ont conduit à l'adoption de la Directive sur la conservation des données de 2006. Concernant le contenu et le champ d'application, la Directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et

[12] Cette disposition fera l'objet ultérieurement de l'interprétation de l'arrêt Tele2 de décembre 2016

[13] Turkalj, K., Borba protiv terorizma na razini Europske unije // Hrvatska pravna revija, 2 (2002), 10; 1-15

[14] 2477ème session du Conseil - JUSTICE AND HOME AFFAIRS - Bruxelles, 19 Decembre 2002; Council Conclusions on Information technologies and the investigation and prosecution of organised crime; doc. 15691/02

[15] Mitsilegas V. (2009.) EU Criminal Law, Oxford and Portland, Oregon

de poursuite d'infractions graves. Par conséquent, l'objectif de la conservation des données est défini de sorte que toutes les infractions criminelles ne sont pas concernées. La Directive définit clairement des critères de conservation des données par les fournisseurs de services tout comme les conditions d'accès à ces données par les autorités, et garantit la protection des données personnelles et la sécurité des données conservées. Elle prévoit l'obligation des fournisseurs de services de collecter les données de trafic et de localisation, ainsi que les données relatives à l'identité de l'abonné ou de l'utilisateur afin d'en garantir l'accès aux autorités à des fins de prévention, de détection, d'enquêtes et de poursuites d'infractions graves, en particulier la criminalité organisée et le terrorisme, laissant le soin de la définition des précédentes notions aux cadres juridiques nationaux. Les données qui doivent être conservées s'appliquent aux données de trafic et de localisation des personnes physiques ou morales ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur inscrit[16]. Les données révélant le contenu des communications ne peuvent être stockées et la conservation des données ne peut s'appliquer que sur une période de 6 mois à 2 ans[17]. La Directive réglemente l'accès à ces données et impose l'obligation aux États membres d'adopter des mesures pour garantir que l'accès ne soit accessible qu'aux autorités nationales compétentes dans des cas spécifiques conformément à la législation nationale et aux exigences de nécessité et de proportionnalité[18]. Enfin, la Directive prévoit expressément des principes de sécurité minimale nécessaires (garanties) qui doivent être fournis par les prestataires tout comme des mesures techniques et organisationnelles visant à empêcher la divulgation ou l'accès non autorisé, la destruction ou la perte accidentelle, la modification ou toute autre forme illégale de traitement. Outre les mesures mentionnées ci-dessus, les États doivent assurer une supervision indépendante de la mise en œuvre des dispositions nationales correspondantes[19].

Dès son entrée en vigueur, la Directive a été vivement critiquée par des associations non-gouvernementales, des fournisseurs de services ainsi que par le contrôleur européen de la protection des données, la qualifiant „*d'instrument probablement le plus irrespectueux de la vie privée des citoyens européens au regard de l'intrusion manifeste qu'il constitue et du nombre élevé de personnes concernées*"[20]. Cette levée de bouclier s'est traduite par de nombreux recours devant les juridictions nationales de la part d'organisations civiles (*Digital Rights Ireland*) et de personnes physiques et morales (*Tele2*) qui remettent en cause la légalité des mesures de conservation des données. Dans ce contexte et suite à la demande de décision préjudicielle présentée par les juridictions nationales, la Cour de justice

[16] Voir: Art. 5. par. 1., op. cit. pp. 54-63

[17] Voir: Art. 5. par. 2. et Art. 6., op. cit. pp. 54-63.

[18] Voir: Art. 4., op. cit. pp. 54-63

[19] Voir: Art. 7 et Art. 9, op.cit pp. 54-63

[20] Concernant les commentaires de Drewry, voir: Drewry, L. (2016) Crimes without culprits: Why the European union needs data retention, and how it can be balanced with the right to privacy. Wisconsin International Law Journal, p. 733

européenne a rendu des décisions fixant un certain nombre de limites au régime de conservation existant.

V. CADRE JURIDIQUE DE LA CONSERVATION DES DONNÉES EN CROATIE

La question de la conservation des données de communication électronique et de l'accès à ces données par les autorités compétentes dans le système juridique de la République de Croatie est encadrée par un certain nombre de dispositions législatives. Dans ce domaine, on note particulièrement la Loi sur les communications électroniques (ci-après: ZEK[21]), le Code de procédure pénale (ci-après: ZKP[22]) ainsi que la Loi sur la sécurité et le renseignement de la République de Croatie (ci-après : ZSOS[23]). En outre, nous pouvons mentionner l'importance de la Loi sur la défense[24], l'Ordonnance sur la police militaire et l'exercice des agents de police militaire[25] ainsi que le Règlement sur les obligations en matière de sécurité nationale pour les personnes morales et physiques croates dans les télécommunications (ci-après: Uredba[26]). Ces dispositions réglementent un certain nombre de questions importantes concernant la conservation des données telles que les périodes de conservation, le périmètre des personnes concernées, les catégories de données et les moyens de communication, l'accès aux données par les autorités compétentes et les garanties de protection.

En ce qui concerne l'objectif de la conservation des données, l'article 339a de la ZEK prévoit l'obligation pour les fournisseurs de services de conserver les données relatives aux communications électroniques afin de faciliter l'enquête, la détection et la poursuite des infractions pénales mais aussi pour assurer les conditions nécessaires à la défense et à la sécurité nationale en vertu d'une réglementation spécifique. Ainsi, dans les normes juridiques, la conservation des données est liée à la commission d'une infraction pénale dont la gravité est déterminée par cette législation spécifique. La réglementation en question qui détermine les infractions pénales pour lesquelles il est possible d'accéder aux données conservées correspond à l'article 339.a de la ZKP de l'année 2014 qui prévoit que les mesures d'instructions, comprenant l'accès aux données conservées, ne peuvent être prises que pour la collecte de preuves concernant les infractions qui permettent d'ordonner l'exécution de mesures spécifiques ainsi que pour les autres infractions exposant à

[21] Zakon o elektroničkim komunikacijama (NN 73/08, 90/11, 133/12, 80/13, 71/14)

[22] Zakon o kaznenom postupku (NN 121/11, 143/12, 56/13, 145/13, 152/14)

[23] Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06, 105/06)

[24] Zakon o obrani (NN 73/13, 75/15, 27/16)

[25] Pravilnik o vojnopolicijskim poslovima i provedbi ovlasti ovlaštenih službenih osoba vojne policije (NN 44/14)

[26] Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama (NN 64/08, 76/13).

des peines d'emprisonnement d'au moins cinq ans[27]. Ainsi, l'accès et l'objectif de la conservation des données se limitent à la détection et à la poursuite des infractions les plus graves.

Le cadre juridique stipulant les types d'informations soumises à l'obligation de conservation des données est contenu dans la ZEK, la ZKP, la ZSOS et l'Uredba. L'article 110 de la ZEK énonce également les types de données liées à l'obligation de conservation, à savoir: les données requises pour la surveillance et la détermination des sources de communication; les données nécessaires pour déterminer la destination de la communication; les données nécessaires pour déterminer la date, l'heure et la durée de la communication; les données nécessaires pour déterminer le type de communication; les données nécessaires pour déterminer le matériel ou le dispositif de communication de l'utilisateur; les données nécessaires pour déterminer la localisation de l'équipement de communication mobile. Les données conservées comprennent également les données relatives aux appels infructueux. L'article 105, paragraphe 4, de la ZEK stipule que les informations établies sur des appels, SMS ou MMS malveillants ou dérangeants doivent être conservées par les fournisseurs de réseaux publics de communication dans le cadre de l'art. 109 et doivent être transmises aux autorités de police dans les plus brefs délais pour suite à donner. Il faut préciser que la loi interdit la conservation des données révélant le contenu de la communication. Par ailleurs, des sanctions sont prévues en cas de non-respect des obligations par les fournisseurs de communications ce qui est considéré comme une violation grave de la ZEK.

La ZKP précise également les types de données conservés lorsqu'elle énonce les conditions d'accès à ces données. Ainsi, l'article 339a de la ZKP stipule que la police peut, sur la base d'un mandat du juge d'instruction, demander au fournisseur de services publics de communications d'avoir accès aux informations concernant le propriétaire enregistré ou l'utilisateur s'il existe un soupçon d'infraction pénale le concernant, notamment pour la vérification d'identité, la détermination de la durée et de la fréquence des communications en fonctions des adresses électroniques ainsi que la localisation et les références de l'appareil et la localisation des personnes l'utilisant.

Dans le cadre juridique national, des mesures avaient déjà été introduites en 2006 concernant la conservation préventive obligatoire de données privées des citoyens dans le cadre de la ZSOS sur la base de laquelle a été adoptée l'Uredba.

La disposition de l'article 21 de l'Uredba prévoit que les personnes morales et physiques qui disposent d'un réseau public de télécommunications et qui fournissent des services publics de télécommunications et des services d'accès sur le territoire de la République de Croatie sont tenues de conserver les catégories suivantes de données nécessaires pour la détection et l'identification des sources de communication ; dans le cas d'un réseau de téléphonie mobile ou fixe : numéro de téléphone fixe ou mobile à l'origine de la communication, nom et prénom, nom de

[27] Voir: ZKP, (NN 152/14)

la personne morale, adresse de l'abonné ou du propriétaire enregistré d'un compte ; dans le cas d'un accès internet : adresse électronique, téléphonie par internet et autres formes de communication de données[28]. La formulation „*et autres formes de communication de données*" pourrait être interprétée comme concernant le contenu même de la communication. Si tel était le cas, cela serait contraire aux obligations découlant de la Directive qui interdit la conservation des contenus de communication.

Les groupes des personnes potentiellement concernés par les mesures de conservation des données est énoncé dans la ZEK et la ZSOS. La formulation de l'article 109 de la ZEK fait référence de manière générale à l'obligation de conserver les données sans préciser le groupe de personnes. En effet, l'accent est mis sur la conservation des données de manière à ce que cette mesure prenne en compte implicitement les données de tous les utilisateurs de communications électroniques. En revanche, la ZSOS prescrit la conservation des données relatives au trafic des télécommunications réalisé par les utilisateurs des services[29].Il découle de cette disposition que la conservation des données s'applique à tous les utilisateurs de communications électroniques. Ainsi, les personnes concernées étant définies de manière générale et sans distinctions, la réglementation s'applique à tous les abonnés et utilisateurs enregistrés, qu'il y ait ou non des indices concernant des activités liés à des infractions pénales graves, et à tous les moyens de communication électroniques et données relatives au trafic.

Concernant la période de conservation des données, l'article 109 de la ZEK stipule que les fournisseurs de services sont dans l'obligation de les conserver 12 mois à compter de la date où la communication a été effectuée. Conformément aux dispositions de l'article 19, paragraphe 5, de la ZSOS, les données de trafic réalisé relatives à l'utilisateur de service sont conservées sur une période d'un an. Il faut interroger ici la durée de la période de conservation pour la poursuite d'infractions pénales graves et se demander si elle ne pourrait pas être plus courte.

En ce qui concerne l'accès des autorités compétentes aux données conservées, des dispositions sont prises dans la ZEK et la ZKP. Ainsi, l'article 109, paragraphe 4, de la ZEK prévoit que les opérateurs de réseaux de communications publics et de services de communications électroniques accessibles au public sont tenus de conserver les données de manière à pouvoir transmettre sans délai les données à l'organisme compétent, à savoir l'OTC (Centre technique opérationnel pour la surveillance des télécommunications).

Jusqu'en 2002, les autorités de police imposaient ses exigences aux fournisseurs de services de télécommunications sur le fondement de de l'article 177, paragraphe 2, de la ZKP qui prévoyait la saisie et „*d'autres mesures et actions nécessaires*"

---

[28] Voir article 21 de l'Uredba, op.cit.

[29] L'article 19, paragraphe 5, de la ZSOS stipule que les personnes physiques et morales qui disposent d'un réseau de télécommunication public et qui fournissent des services de télécommunication publics et des services d'accès en Croatie sont tenues de conserver les données de trafic realisé par l'utilisateur de service durant un an.

afin de faciliter les enquêtes sur les infractions faisant l'objet de poursuites à la diligence du ministère public. La modification de la loi en 2002 permet à la police dans le cadre d'une enquête d'infraction pénale d'identifier les adresses électroniques d'une connexion sur une période donnée. La Loi sur la police stipule que la police , sur la base de l'accord écrit du chef de la police criminelle ou du chef du bureau de la police national pour la lutte contre la corruption et le crime organisé ou le chef de l'administration de police, peut exiger du fournisseur de services de communications la vérification de l'identité, la durée et la fréquence des communications de certaines adresses électroniques si cela est nécessaire pour la prévention et la détection d'infractions pénales faisant l'objet de poursuites à la diligence du ministère public et leurs auteurs, réduire le risque et la violence, rechercher les personnes et les objets.

En octobre 2013, grâce à un complément apporté à une disposition de l'article 339 de la ZKP (NN 145/13) qui permet d'avoir accès aux contacts établis lors des communications électroniques, les mesures d'instructions sont réglementées ce qui représente un progrès dans la protection de la vie privée du propriétaire ou de l'utilisateur des dispositifs de communication. Comme indiqué ci-dessus, suivant la réglementation précédente, il s'agissait d'une enquête de l'autorité de police. Considérant les ingérences que cela implique sur les droits fondamentaux, significativement plus importantes que dans d'autres types d'enquêtes, dans le cadre de l'accès aux contacts établis lors de communication afin de collecter des preuves et de détecter les criminels relevant d'infractions pénales poursuivies d'office, le législateur a décidé de modifier la ZKP dans le but de renforcer le degré de la protection des droits fondamentaux des propriétaires ou utilisateurs d'équipements de télécommunication, notamment le droit à la vie privée.

Une garantie supplémentaire est apportée par une nouvelle disposition de 2014 de l'article 339 de la ZKP[30] qui limite le champ d'action de la collecte de preuves à partir des contacts de télécommunication électronique de manière à ce que la collecte de preuves ne puisse être effectuée que pour des infractions pénales pour lesquelles il est possible de prendre des mesures d'instructions spécifiques ainsi que pour les infractions pénales passibles d'une peine d'emprisonnement de plus de cinq ans, et non plus pour celles dont la procédure pénale est engagée d'office. En effet, compte tenu du degré d'intrusion dans la vie privée des individus concernés, il s'est révélé nécessaire de limiter la capacité d›accéder à ces données et leur utilisation seulement aux crimes les plus graves pour lesquels une telle ingérence peut être justifiée. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne établit des mécanismes de protection garantissant le respect de la vie privée et la protection des données à caractère personnel en cas de conservation des données, notamment un mécanisme de sauvegarde limitant l'accès aux données conservées et leur utilisation. La modification de la ZKP la rend conforme à ces principes.

Le pouvoir d'initier une vérification des contacts de télécommunication établis dépend de l'enregistrement ou non par l'opérateur du propriétaire ou utilisateur

[30] Voir: ZKP, (NN 152/14)

concerné par la mesure. L'application de cette mesure ne peut être effective que pour le propriétaire ou utilisateur du moyen de communication que l'on soupçonne d'avoir commis un crime pour lequel la procédure pénale est engagée d'office. Cette action permet de : a) identifier le dispositif utilisé, b) contrôler les contacts établis ce qui implique la vérification de l'identité ainsi que la durée et la fréquence des communications, c) localiser les personnes ayant établi la communication électronique, d) localiser le dispositif de communication indépendamment de l'établissement du contact de télécommunication.

La disposition de l'article 339 de la ZKP énonce que la police peut, sur la base d'un mandat du juge d'instruction, exiger du fournisseur de services de communications publiques des informations concernant le propriétaire enregistré ou l'utilisateur du moyen de télécommunication soupçonné d'avoir commis une infraction pénale, à savoir la vérification de l'identité, la durée et la fréquence des communications liées à certaines adresses électroniques, la localisation du dispositif de communication, la localisation des personnes à l'origine de la communication électronique, la référence et l'identifiant de l'appareil. Les mêmes vérifications peuvent être ordonnées pour une personne en lien avec une personne soupçonnée d'être l'auteur d'une telle infraction pénale. Le mandat est délivré par le juge d'instruction sur la base d'une proposition initiée par le procureur de l'état compétent.

La ZKP énonce un critère clair et objectif qui indique quelles infractions sont susceptibles de permettre l'accès aux données conservées. Elle garantit le contrôle judiciaire dans cette procédure ainsi que l'utilisation de ces données conformément aux fins prescrites. Egalement, il est clairement mentionné que les données obtenues sans mandat approprié du juge d'instruction ne peuvent être utilisées comme éléments de preuve dans la procédure. En outre, les dispositions de la ZKP prévoient l'information des personnes dont les données sont conservées puisque les articles 183,184 et 184a de ladite loi énoncent que le prévenu dispose du droit d'accéder au dossier.

Au sujet des garanties de sécurité et de la protection des données conservées, la disposition de l'article 109, paragraphe 5, de la ZEK prévoit spécifiquement les principes de sécurité des données conservées que les fournisseurs de services sont tenus de respecter: les données conservées doivent être protégées de manière appropriée de la destruction accidentelle ou illégal ; de la perte ou l'altération accidentelle ; du stockage, du traitement, de l'accès ou de la divulgation qui sont non autorisés ou illégaux ; l'accès aux données conservées doit être limité aux personnes autorisées et aux autorités compétentes qui ont le droit d'accéder à ces données ; les données conservées doivent être détruites après expiration de la période de rétention sauf exception ; les fournisseurs de services doivent assurer à leurs propres frais, et mettre en œuvre, tous les dispositifs techniques et organisationnels nécessaires au respect des principes de sécurité énoncés. Conformément aux dispositions de la Directive 2002/58, les fournisseurs de services doivent, par des mesures techniques et organisationnelles appropriées, garantir la protection efficace des données conservées contre les risques d'utilisation abusive et d'accès non autorisée à ces

données. Ils doivent garantir la pleine intégrité et la confidentialité des données et un haut niveau de protection et de sécurité.

Afin de garantir le respect des règles relatives à la conservation des données, le législateur a également prévu une responsabilité contraventionnelle pour les fournisseurs de services. Les opérateurs peuvent être condamnés à une amende conformément à la disposition de l'article 118 de la ZEK si ils ne remplissent pas leurs obligations.

VI. ARRÊTS DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE SUR LA CONSERVATION DES DONNÉES

Suite aux attentats terroristes commis aux États-Unis, au Royaume-Uni et en Espagne, les politiques de l'Union se concentrent sur le renforcement de la sécurité au détriment des droits et libertés fondamentaux. On assiste alors à l'apparition d'une distorsion entre les demandes de respect des droits de l'homme et les besoins de sécurité. Par la suite, un équilibre précaire a été retrouvé progressivement en mettant davantage l'accent sur la protection des droits de l'homme. La Cour de justice de l'Union européenne, par ses arrêts, a apporté un certain nombre de correctifs dans l'objectif de lutter contre le terrorisme sur le territoire d l'Union. En effet, la Cour européenne a déjà rendu plusieurs arrêts qui ont eu un impact significatif sur la protection des droits de l'homme parallèlement à la mise en œuvre de la politique antiterroriste de l'Union européenne. En premier lieu, il faut mentionner un certain nombre d'arrêts rendus suite à des mesures restrictives spécifiques prises à l'encontre de personnes ou d'entités pour leur implication dans le financement du terrorisme. Le plus significatif d'entre eux est probablement l'arrêt de la Cour (grande chambre) du 3 septembre 2008 par lequel celle-ci constate une violation du droit de propriété et annule le règlement dans la mesure où il concerne M. Kadi[31]. Suite aux considérations de la Cour dans l'affaire Kadi, la Cour a également réformé le jugement de première instance dans l'affaire Hassan et a annulé le règlement (CE) no 881/2002 dans la mesure où il concerne Hassan et Ayadi[32]. La Cour a estimé que le droit à la défense et le droit à une protection juridictionnelle effective n'avaient pas été respectés dans ces affaires[33]. En outre, la Cour a conclu à la violation du droit de propriété par l'application de mesures de gel de fonds qu'elle considère comme des restrictions injustifiées en la matière[34]. Ce développement a été renforcé par

[31] Arrêt de la Grande Chambre du 3 Septembre 2008 dans les affaires jointes C-402/05 P et C-415/05 P Yassin Abdullah Kadi et Al Barakaat International Foundation contre le Conseil de l'Union européenne avec le soutien de l'Espagne, la France, les Pays-Bas et la Commission européenne, Recueil de la jurisprudence de la Cour 2008, p. 1-06351.

[32] Arrêt de la Cour du 3 Décembre 2009 dans l'affaire C-399/06 P et C-403/06 P, Hassan contre le Conseil de l'Union européenne et la Commission européenne et Ayadi contre le Conseil de l'Union européenne, Recueil de la jurisprudence de la Cour, 2009.

[33] Ibid., par. 84-86.

[34] Ibid., par. 93.

deux arrêts pris par la Cour de l'UE concernant la conservation des données qui ont une importance capitale dans l'édification d'une future réglementation de protection des données tant au niveau de l'Union que national. Il s'agit des arrêts *Digital Rights* de 2014 et *Tele2* de 2016.

Dans l'arrêt *Digital Rights,* la Cour a abrogé la Directive 2006/24/CE relative à la conservation des données. Le jugement était rendu suite aux demandes de décision préjudicielle issues des juridictions autrichienne[35] et irlandaise[36]. La demande déposée par la juridiction irlandaise en juin 2012 était relative à la légalité des mesures législatives et administratives nationales concernant la conservation des données des communications électroniques alors que la demande présentée par la juridiction autrichienne en décembre 2010 était liée au recours constitutionnels au sujet de la compatibilité de loi transposant la Directive 2006/24 dans le droit interne autrichien avec la loi constitutionnelle fédérale.

Plus précisément, les deux demandes de renvoi préjudiciel se rapportent à la question de la compatibilité de la Directive 2006/24 sur la conservation des données avec le droit au respect de la vie privée et des communications visé par l'article 7 de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée Charte), le droit à la protection des données à caractère personnel visé par l'article 8 et le droit à la liberté d'expression en vertu de l'article 11. Ainsi, la question est de savoir si la Directive 2006/24 est conforme à la Charte dans la mesure où elle permet de stocker une grande quantité de données d'un nombre illimité de personnes sur une longue période. De plus, dans la plupart des cas le comportement des personnes concernées ne justifie pas de telles mesures prises à leur encontre.

Comme l'indique la motivation de l'arrêt, la Cour européenne considère que la Directive 2006/24 sur la conservation des données ne prévoit pas de règles claires et précises pour réglementer les possibilités d'ingérence dans les droits fondamentaux des articles 7 et 8 de la Charte. Plus précisément, il n'y est pas prévu de limites qui garantiraient que l'ingérence se réduit à ce qui est strictement nécessaire . La Cour estime également que la Directive n'énonce pas de critères clairs concernant l'accès à ces informations et ne prévoit pas de garanties suffisantes pour la protection des données à caractère personnel et la sécurité des données conservées[37].

La Cour estime que l'ingérence dans le droit au respect de la vie privée et des communications se reflète dans le fait que les données conservées permettent de prendre connaissance des personnes avec lesquelles un abonnée ou un utilisateur inscrit a communiqué et par quel moyen, connaître la durée et la localisation de la communication. Ces données fournissent également des informations concernant

---

[35] Plus de détails dans C-594/12 Demande de décision préjudicielle formulée par le Verfassungsgerichtshof (Autriche) du 19 Decembre 2012 – Kärntner Landesregierung and Others, OJ C 79, 16 mars 2013

[36] Plus de détails dans C-293/12 Demande de décision préjudicielle présentée par la High Court of Ireland , le 11 juin 2012- Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, OJ C 258, 25 août 2012

[37] Voir le point 65 de l'arrêt

la fréquence des communications avec certaines personnes au cours d'une période donnée. Prises dans leur ensemble, elles permettent aussi d'obtenir des informations très précises sur la vie privée des personnes: habitudes de la vie quotidienne, lieux de résidences permanents ou temporaires, habitudes de déplacements, relations sociales et milieux sociaux fréquentés[38]. L'accès des autorités à ces informations constituent donc une intrusion manifeste dans l'intimité des personnes et va à l'encontre de leurs droits fondamentaux. Cela entraîne par conséquent une ingérence dans le droit à la liberté d'expression garanti par l'article 11 de la Charte dans la mesure où cela peut dissuader les individus d'utiliser les réseaux de communication[39]. L'atteinte au droit à la protection des données à caractère personnel est donc caractérisée par le fait que la conservation des données se traduit par le traitement de celles-ci.

À propos de la justification de l›ingérence dans les droits fondamentaux, la Cour estime que toute restriction des droits et libertés n›est justifiée que dans la mesure où elle est nécessaire et qu'elle répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui[40]. La Cour est consciente que par la conservation des données on n'autorise pas l'accès au contenu des communications électroniques, mais uniquement aux données de trafic et de localisation, et que les fournisseurs de services doivent respecter les principes de protection et de sécurité des données. Cependant, la Cour, qui ne conteste pas que la lutte contre la criminalité grave, notamment la lutte contre le crime organisé et le terrorisme, constitue une priorité pour la sécurité publique[41], considère pourtant qu'un tel objectif relevant de l'intérêt général, ne peut justifier la nécessité des mesures de conservation telles qu'elles sont prévues dans la Directive. La Cour considère que la Directive susmentionnée englobe de manière générale toutes les personnes et tous les moyens de communication électronique, ainsi que toutes les données relatives au trafic, sans distinction, restriction ou exception en ce qui concerne la lutte contre les infractions pénales graves. La Directive fait généralement référence à toutes les personnes utilisant des services de communications électroniques, y compris celles qui, même indirectement, ne sont pas dans un cas de figure susceptible d'entraîner des poursuites. Elle s'applique donc à des personnes pour lesquelles rien n'indique qu'elles puissent être liées, de près ou de loin, à des infractions graves et elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un groupe de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves[42].

Au sujet de l'accès aux données conservées, la Directive ne prévoit aucun critère objectif qui permettrait de limiter l'accès aux données des autorités nationales

[38] Voir les points 26 et 27 de l'arrêt
[39] Voir point 28 de l'arrêt
[40] Voir point 38 de l'arrêt
[41] Voir point 51 de l'arrêt
[42] Voir points 57 et 58 de l'arrêt

compétentes et de restreindre leur utilisation ultérieure à des fins de prévention, de détection ou de poursuite. En outre, la Directive ne prévoit pas de limitation stricte de l'accès aux données et de leur utilisation ultérieure aux fins de la prévention et de la détection d'infractions pénales graves, mais indique seulement que chaque État membre doit fixer la procédure et les conditions à respecter conformément aux exigences de nécessité et de proportionnalité[43] pour accéder aux données conservées. Les critiques pointent également du doigt le fait que l'accès des autorités nationales compétentes aux données conservées n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire. Enfin, s'agissant de la période de conservation, la durée prévue est de six à 24 mois.

En raison de l'invalidation de la Directive sur la conservation des données, il n'existe plus de cadre juridique, au niveau de l'Union, qui réglemente le domaine de la conservation des données de communications électroniques. Dans la mesure où la législation nationale dans ce domaine est toujours en vigueur (soit elle est restée inchangée soit elle a été modifiée conformément à la jurisprudence de la Cour de justice de l'UE), la question de la conformité de ces solutions nationales avec la réglementation de l'UE a été soulevée.

À la suite de l'arrêt *Digital Rights*, en Suède, *Tele2 Sverige* a décidé de conformer ses actions avec les exigences du jugement et a informé par conséquent les autorités nationales que la société cesserait de conserver les données relatives aux communications électroniques et qu'elle supprimerait les données précédemment conservées. Le Rapporteur spécial du Ministre suédois de la justice a analysé les dispositions relatives à la conservation des données et a émis un avis selon lequel elles ne s'opposaient ni au droit de l'Union ni à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, à savoir que l'arrêt *Digital Rights* ne peut être interprété comme limitant le principe de conservation généralisée et indifférenciée des données lui-même[44]. À la suite d'un tel avis, les autorités compétentes ont demandé à *Tele2* de se conformer aux mesures de conservation des données. Considérant que la conclusion du Rapporteur spécial repose sur une interprétation erronée de l'arrêt *Digital Rights* et que l'obligation de conserver les données est contraire aux droits fondamentaux garantis par la Charte, *Tele2 Sverige* a intenté une action en justice contre l'ordonnance de conservation des données. Dans le cadre de cette procédure, le tribunal pose une question préjudicielle, à savoir si l'article 15, paragraphe 1, de la Directive 2002/58, lu conjointement avec les articles 7 et 8 et l'article 52, paragraphe 1, de la Charte, doit être interprété comme s'opposant à une réglementation nationale qui, aux fins de

[43] Voir points 61 et 62 de l'arrêt

[44] Il conteste l'interprétation de l'arrêt Digital Rights selon laquelle la Cour y définirait un certain nombre de critères à respecter pour pouvoir considérer une réglementation comme étant proportionnée. Il conviendrait d'apprécier toutes les circonstances afin de déterminer la conformité de la réglementation suédoise au droit de l'Union, telle que l'ampleur de la conservation des données au regard des dispositions sur l'accès aux données, sur la durée de leur conservation, sur leur protection ainsi que sur leur sécurité

la lutte contre la criminalité, prévoit la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électroniques[45].

Le renvoi préjudiciel adressé à la Cour de justice de l'Union au mois de décembre 2015 par la juridiction anglaise de deuxième instance (appel), résulte de la demande de certaines personnes physiques de contrôler la légalité ou la conformité des réglementations nationales sur la conservation des données avec le droit de l'Union européenne. Selon le tribunal de première instance, la Cour de justice ayant estimé que la Directive 2006/24 était incompatible avec le principe de proportionnalité, une disposition nationale dont le contenu serait identique n'est également pas compatible avec ce principe. Le ministre de l'Intérieur a interjeté un appel contre ce jugement et la Cour d'appel a envoyé un renvoi préjudiciel visant à déterminer si l'arrêt *Digital Rights* établit des exigences impératives en droit de l'Union, applicables au régime national d'un État membre régissant l'accès aux données conservées conformément à la législation nationale, afin de se conformer aux articles 7 et 8 de la Charte. L'arrêt *Digital Rights* étend-il la portée des articles 7 et/ou 8 de la Charte au-delà de celle de l'article 8 de la CEDH, telle qu'établie par la jurisprudence de la Cour européenne des droits de l'homme ? La Cour de justice a jugé cette question irrecevable, estimant que la question précitée ne saurait affecter l'interprétation de la directive 2002/58, c'est-à-dire que la réponse à cette question ne saurait fournir des éléments d'interprétation du droit de l'Union

Enfin, en décembre 2016, la Cour de justice de l'Union européenne a rendu l'arrêt *Télé2* donnant un avis sur la conformité des dispositions nationales relatives à la conservation des données avec les dispositions de l'art. 15-I de la Directive 2002/58 / CE sur la vie privée et les communications électroniques. Comme il est indiqué dans les motivations du jugement, la Cour de l'Union européenne estime que la réglementation nationale qui, en vue de lutter contre la criminalité, prévoit la conservation généralisée et indifférenciée de toutes les données de trafic et de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique est contraire aux dispositions de l'article 15, paragraphe 1, de la Directive 2002/58 / CE sur la vie privée et les communications électroniques, ainsi que celles prévues par une réglementation nationale prévoyant la protection et la sécurité des données de trafic et de localisation et en particulier l'accès aux données conservées par les autorités nationales compétentes lorsque l'objectif de cette approche dans la lutte contre la criminalité ne se limite pas à la lutte contre les infractions pénales graves, lorsque cet accès n'est pas soumis au contrôle préalable d'une juridiction ou d'un organe administratif indépendant et lorsqu'il n'est pas prescrit que les données en question restent sur le territoire de l'Union[46].

[45] Pour plus de détails voir dans C-203/15: Request for a preliminary ruling from the Kammarrätten i Stockholm (Suède), OJ C 221, 6 mai 2015

[46] Voir dispositif de l'arrêt, points 1 et 2

La Cour de l'Union européenne relève notamment qu'un des objectifs de la Directive est de respecter les droits énoncés aux articles 7 et 8 de la Charte et qu'il est apparent que le législateur européen souhaite qu'un niveau élevé de protection des données à caractère personnel et de la vie privée soit toujours garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée. Dans ce but, la Directive 2002/58 contient des dispositions spécifiques visant à protéger les utilisateurs des services de communications électroniques contre les risques pour les données à caractère personnel et la vie privée résultant des nouvelles technologies et de la capacité accrue de stockage et de traitement automatisé de données[47].

La Cour reconnaît que si la disposition de l'article 15, paragraphe 1, de la Directive autorise des exceptions dans les obligations des États membres de garantir aux citoyens de l'Union la confidentialité des communications et donc de leurs données personnelles, il n'en demeure pas moins que l'existence d'un régime de conservation généralisée et indifférenciée de toutes les données de trafic et de localisation et de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électroniques, qui est effectué systématiquement et de façon continue, devient la règle et non l'exception comme la Directive l'exige[48]. Une telle conservation des données ne prévoit aucune distinction, restriction ou exception par rapport au but à atteindre. Elle s'applique généralement à toutes les personnes utilisant des services de communications électroniques sans que celles-ci soient, même indirectement, dans une situation pouvant donner lieu à des poursuites pénales. Cette conservation dépasse les limites strictement nécessaires et ne peut être considérée comme justifiée dans une société démocratique. La Cour rappelle que la disposition de l'article 15, paragraphe 1, de la Directive prévoit elle-même qu'une mesure s'écartant du principe de la confidentialité des communications et des données liées de trafic n'est autorisée que si elle se révèle nécessaire et s'applique de manière appropriée et proportionnée dans le cadre d'une société démocratique. Autrement dit, elle doit être strictement proportionnée à son objectif. La même disposition prévoit également que la conservation des données s'effectue sur une période limitée en conformité avec les objectifs prescrits (sauvegarde de la sécurité nationale, de la défense et de la sécurité publique ainsi que mise en œuvre de la prévention, de la recherche, de la détection et de la poursuite des infractions pénales).

La Cour souscrit aux considérations de l'arrêt *Digital Rights* selon lesquelles la conservation des communications électroniques peut permettre de tirer des conclusions très précises sur la vie privée de la personne dont les données sont conservées. Elle considère avec une gravité particulière le fait que la conservation des données se fasse sans en informer les personnes concernées ce qui peut contribuer à créer chez eux le sentiment que leur vie privée est soumise à une surveillance permanente.

---

[47] Voir le point 82 de l'arrêt

[48] Voir les points 88 et 89 de l'arrêt

VII. CONSÉQUENCES DE LA JURISPRUDENCE SUR LE CADRE JURIDIQUE DE LA CONSERVATION DES DONNÉES DANS L'UNION EUROPÉENNE

En prononçant l'arrêt *Digital Rights* en 2014, par lequel la Directive sur la conservation des données a été abrogée, celle-ci a été supprimée du système juridique de l'Union. La conséquence est qu'il n'existe plus, au niveau de l'UE, de règlement établissant des règles communes dans le domaine de la conservation des données, c'est-à-dire qu'il n'existe pas de règles claires et précises régissant la conservation des données et l'accès des autorités compétentes à ces données et qu'il n'y a, de ce fait, pas de garanties suffisantes permettant une protection efficace des données personnelles contre le risque d'abus. Cependant, cela ne signifie pas que, au niveau de l'Union, il n'y a pas de dispositions concernant la conservation des données. En effet, l'article 15, paragraphe 1, de la Directive sur la vie privée et les communications électroniques, ainsi qu'un certain nombre de dispositions de la Charte des droits fondamentaux sont toujours en vigueur. La Directive étant, de par sa nature, une règlementation que les États membres mettent en œuvre dans leurs législations nationales, les États membres ont adopté des dispositions nationales transposant la Directive sur la conservation des données dans les ordres juridiques respectifs. Par conséquent, après que la Cour a constaté que la Directive sur la conservation des données atteint les droits et libertés fondamentaux, la question de la viabilité des dispositions juridiques nationales sur la conservation des données transposées dans l'ordre juridique national a été soulevée. La question a été posée de savoir dans quelle mesure les réglementations nationales contreviennent aux droits et libertés fondamentaux et s'ils sont contraires à la réglementation en vigueur de l'Union européenne. Après l'arrêt *Digital rights*, sans cadre juridique commun, les législations nationales ont commencé à prendre des dispositions juridiques différentes en matière de conservation des données ce qui a eu pour conséquence l'apparition d'un cadre juridique hétérogène dans ce domaine.

En raison de l'absence de réglementation au niveau de l'UE, les règles et les politiques de conservation des données dans l'Union européenne ont commencé à se développer dans trois directions différentes. Dans certains États (Autriche, Slovénie et Pays-Bas), les cours constitutionnelles ont annulé la réglementation nationale dans le champ de la conservation des données, c'est à dire que celle-ci, en la matière, n'est plus applicable. Certains pays (Belgique, Allemagne, Bulgarie, Roumanie, Slovaquie et Royaume-Uni) ont adopté une nouvelle réglementation et en Irlande et Suède le processus est en cours d'adoption. Les autres pays (Croatie, Chypre, République tchèque, Danemark, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Luxembourg, Malte, Portugal, Pologne, Espagne, Estonie, Finlande) ont conservé les réglementations existantes en prévision de nouveaux régimes au niveau de l'Union. Il en résulte, pour les citoyens de l'Union, une situation d'insécurité juridique dans un contexte où coexistent différents régimes juridiques de conservation des données

en contradiction avec les principes de l'Union Européenne qui se veut un comme un espace de liberté, de sécurité et de justice[49].

La deuxième conséquence importante de ces deux arrêts de la Cour de justice de l'Union européenne est qu'ils ont défini des normes et des hypothèses auxquelles les réglementations nationales doivent se conformer pour réglementer le domaine de la conservation des données. Notamment, la Cour de justice européenne ne conteste pas la nécessité et la justification de la collecte et du traitement des données de communications électroniques. Elle permet ainsi aux États membre d'adopter des règles répondant à certaines conditions concernant la conservation des données et leur accès, la période de conservation et les garanties de protection[50]. La Cour de l'UE énonce clairement les critères auxquels les réglementations nationales doivent se conformer pour ne pas porter atteinte de manière disproportionné aux droits fondamentaux. Les conditions à remplir sont les suivantes:

1.) La conservation des données doit être limitée et la durée proportionnée

Il est nécessaire de limiter la conservation des données relatives au trafic et des données de localisation à des fins de lutte contre la criminalité grave et à condition que la conservation des données 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.

2.) L'accès et l'utilisation des données conservées doivent être limités

Il est nécessaire de définir les circonstances et les conditions permettant l'accès des autorités aux données. L'accès peut être accordé aux fins de la lutte contre la criminalité et uniquement aux données des personnes soupçonnées d'avoir commis une infraction pénale grave ou d'avoir l'intention de la commettre ou d'avoir participé d'une manière ou d'une autre à l'exécution d'une telle infraction. Il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné au contrôle préalable d'une juridiction ou d'une entité administrative indépendante. Il est également important que les autorités nationales compétentes qui ont eu accès à ces informations informent les personnes dont les données sont en cours de traitement, dès lors que cela ne compromet pas l'enquête.

3.) Protéger contre d'éventuels abus

Les fournisseurs de services doivent prendre les mesures techniques et organisationnelles appropriées pour assurer la protection efficace des données

[49] Les données sont issues des des travaux du groupe de travail du Conseil de l'UE sur l'échange d'informations et la protection des données, dont les détails sont confidentiels et limités aux membres du groupe de travail

[50] Arrêt de la Cour de l'UE du 21 Décembre 2016, dans les affaires jointes C-203/15 et C-698/15 (Télé2); Pts. 108-123

conservées contre les risques d'utilisation abusive et d'accès non autorisé à ces données.

En ce qui concerne le cadre juridique de la République de Croatie sur la question de la conservation des données, les conséquences des arrêts qui ont été pris se reflètent dans la pertinence des questions examinées par la Cour sur sa conformité avec les dispositions prises dans ses arrêts. Compte tenu de ce qui précède, la disposition de l'article 109 de la ZEK, qui prescrit la conservation généralisée et indifférenciée des données concernant toutes les personnes qui utilisent des réseaux et des services de communication et cela même si leur comportement ne démontre aucun lien, comme l'exige la Cour, indirect ou distant, avec des infractions pénales graves, est controversé. En ce sens, la disposition de l'article 19, paragraphe 5, de la ZSOS est également contestable car elle prévoit l'application de la mesure de conservation des données sur le trafic de télécommunication réalisée pour tous les utilisateurs du service. Rappelons que la Cour de l'Union ne s'oppose pas à ce qu'un État membre adopte un règlement permettant une conservation ciblée des données qui, en termes de catégories de données et de communication, se limite au strict nécessaire. Par contre, la conservation générale et indifférenciée des données de tous les utilisateurs de communications électroniques va au-delà des limites strictement nécessaires et ne peut être considérée comme justifiée dans une société démocratique, comme l'énonce l'article 15, paragraphe1, de la Directive 2002/58, en lien avec les articles 7, 8 et 11 de la Charte. Aussi, selon la jurisprudence de la Cour européenne, la durée de conservation doit être limitée à ce qui est strictement nécessaire. Compte tenu de ce qui précède, les dispositions de la ZEK et de la ZSOS, qui prescrivent une période de conservation obligatoire d'un an, sont contestables et demanderaient à être réexaminées en prenant en compte l'aspect de stricte nécessité. La Cour de l'UE a établi des critères clairs d'accès aux données qui prescrivent que la législation nationale doit être fondée sur des critères objectifs pour définir les circonstances et les conditions justifiant l'accès des autorités compétentes aux données conservées. Il est également essentiel que l'accès aux données fasse l'objet d'un contrôle préalable par une juridiction ou une autorité administrative indépendante et que les autorités compétentes informent la personne concernée de la mesure de conservation dès lors que cette information ne compromet pas le bon déroulement de l'enquête. Ainsi, les dispositions de la ZKP, qui prévoit cependant le droit pour la personne mise en examen de consulter le dossier, sont questionnables concernant leur conformité avec l'exigence établie par la Cour qui vise à ce que les personnes soient informées lorsque leurs données sont conservées[51]. Une situation particulièrement sensible se pose pour les fournisseurs de services qui, conformément aux dispositions de l'article 118 de la ZEK, sont passibles de sanctions s'ils ne remplissent pas leurs obligations de conserver les données de communication électronique et se retrouve ainsi contraint de violer le droit de l'UE. Pour cette raison, il est nécessaire d'établir un cadre clair permettant aux fournisseurs de services de s'assurer de la légalité de leur action.

[51] Il s'agit des articles 183,184 et 184a de la ZKP

VIII. CRÉER UN CADRE ADAPTÉ POUR UN RÉGIME DE CONSERVATION DES DONNÉES CONFORME AUX DROITS FONDAMENTAUX DES CITOYENS DE L'UNION EUROPÉENNE

La Commission européenne a exprimé son point de vue sur la réglementation concernant la conservation des données au niveau national après l'abrogation de la Directive par la Cour de l'UE. Comme l'a relevé la Commission européenne[52], les États membres sont libres de conserver la législation nationale existante ou d'en introduire de nouvelles, à condition qu'elles soient compatibles avec les sources primaires et secondaires du droit communautaire[53]. Ainsi, la Commission européenne a rappelé qu'il existe des réglementations primaires et secondaires qui réglementent les questions pertinentes liées à la conservation et à l'accès aux données. La législation primaire repose sur les traités fondateurs et la Charte des droits fondamentaux de l'Union européenne garante de la protection des droits de l'homme, tandis que les sources secondaires concernent principalement la Directive 2002/58 / CE sur la vie privée et les communications électroniques.

Compte tenu de l'importance incontestable de la conservation des données dans la lutte contre le terrorisme et les infractions graves d'une part, et de la nécessité de protéger les droits et libertés fondamentaux des citoyens d'autre part, il convient d'examiner les moyens d'améliorer le système de conservation des données proportionnellement à son atteinte éventuelle sur les droits des citoyens de l'UE dans l'esprit des considérations de la Cour de justice européenne.

En ce qui concerne l'admissibilité et la nécessité du régime de conservation des données, il convient de mentionner l'opinion de l'avocat général Henrik Saugmandsgaard Øe du 19 juillet 2016, dans les affaires qui ont conduit à l'arrêt *Tele2*. En effet, citant le considérant 11 de la Directive sur la conservation des données, selon lequel la Directive n'affecte pas la faculté que possèdent les États membres de procéder à l'interception légale des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire et proportionné pour assurer la sauvegarde des objectifs visés ci-dessus, conformément à la Charte des droits fondamentaux de l'Union européenne et à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, l'avocat général estime que l'intention du législateur de l'Union n'était pas d'affecter le droit des États membres d'adopter des mesures de conservation des données, mais que ce droit est soumis à certaines exigences qui concernent notamment les objectifs et la proportionnalité des mesures. En d'autres termes, l'avocat général considère que l'obligation générale de conserver les données en tant que telles ne doit pas être considérée comme toujours dépassant les limites du strict nécessaire dans la lutte contre les infractions pénales

[52] European Commission statement on national data retention laws; STATEMENT/15/5654; Bruxelles, 16 Septembre 2015

[53] Par les dispositions relatives à la protection des droits de l'homme, les directives qui traitent de la question de la protection des données personnelles, ainsi que par la disposition de l'article 15-I de la Directive 2002/58 / CE sur les communications électroniques et la vie privée, la Cour européenne de justice dans son arrêt *Tele2* a interprété la législation nationale relative à la conservation des données

graves, mais que cette obligation dépasse ce qui est strictement nécessaire si elle n'est pas accompagné de garanties concernant l'accès aux données, la durée de conservation, la protection et la sécurité des données. Pour évaluer la nécessité, l'avocat général est d'avis qu'il est nécessaire d'examiner si d'autres mesures seraient aussi efficaces qu'une obligation générale de conservation dans la lutte contre les infractions graves, compte tenu du fait que ces mesures donnent aux autorités compétentes la possibilité d'avoir, par l'examen des données, accès au passé[54].

En raison de l'absence d'une approche uniforme au niveau européen, sans prescriptions de standards minimaux visant à aligner les réglementations des États membres relatives aux obligations de conservation des données de communication électronique, il est d'autant plus nécessaire d'adopter un règlement au niveau européen qui garantirait que les États membres ont une approche uniforme de la question de la conservation des données, dans le plein respect des droits des citoyens de l'UE garantis par la Charte. Un tel cadre juridique uniforme contribuerait non seulement à l'harmonisation des législations nationales dans le domaine de la conservation des données en réduisant les différences juridiques entre eux, mais supprimerait également les risques de violation des droits européens énoncés par la Charte par des dispositions nationales. La nouvelle directive devrait protéger les droits de la vie privée garanti aux citoyens de l'UE grâce à la mise en place d'un cadre clair à la conservation des données (et à leur accès) afin de lutter contre le terrorisme et la criminalité grave.

Nous pouvons trouver un exemple récent de solution nationale à la question de la conservation des données dans la législation allemande qui a été adoptée en décembre 2015 et est entré en vigueur en juillet 2017 (cette longue vacatio legis a été prescrite afin de laisser le temps d›adaptation nécessaire aux fournisseurs de services pour adopter le nouveau régime de conservation des données). La nouvelle réglementation allemande établit une distinction claire entre l'obligation de conserver les données et l'accès aux données. La période de conservation des données a été réduite à quatre semaines par rapport aux données de localisation (du fait de leur sensibilité) et à dix semaines par rapport aux données de trafic. En ce qui concerne les données de trafic, certaines catégories de ces données ne peuvent être obligatoirement détenues, comme toutes les données de courrier électronique et les informations sur les sites visités, ainsi que les données relatives au fonctionnement des organisations sociales et religieuses qui offrent des conseils par téléphone. Par conséquent, l'Allemagne n'a pas réduit en substance le groupe des personnes dont les données sont conservées, mais elle a raccourci la période de conservation des données et a exclu certaines catégories de données susceptibles d'être conservés. Ainsi, l'Allemagne n'a pas répondu pleinement aux exigences de la Cour concernant la sélection des personnes dont les données sont conservées.

[54] Avis de l'avocat général Henrik Saugmandsgaard Øe dans les affaires jointes C-203/15 Tele2 Sverige AB / Post-och telestyrelsen et C-698/15 secrétaire d'État aux affaires intérieures / Tom Watson et al. du 19 juillet 2016; p. 29

En ce qui concerne l'accès aux données, il n'est possible que dans les cas d'enquêtes pour des infractions pénales graves et pour prévenir des menaces graves contre l'intérêt public. L'accès aux données diffère suivant qu'il s'agisse de données conservées par les fournisseurs de services à des fins professionnelles (données de facturation) ou de données que les fournisseurs conservent par obligation. Les requérants ne peuvent accéder aux données sur le trafic que si la personne est soupçonnée d'avoir commis une des infractions graves suivantes : création d'une organisation terroriste, distribution de pédopornographie, meurtre, traite d'êtres humains à des fins d'exploitation sexuelle. L'accès aux données est possible uniquement sur la base d'une décision de justice et uniquement à des données relatives aux personnes soupçonnées ou accusées d'avoir commis des infractions pénales, à condition que cet accès leur soit notifié. Les données conservées doivent être détruites dès qu'elles ne sont plus nécessaires dans le cadre des poursuites pénales. La nouvelle réglementation allemande a été adoptée après l'arrêt *Digital Rights*, mais avant l'arrêt *Tele2*, et n'a donc pas répondu pleinement aux exigences et aux normes fixées par la Cour en matière de conservation des données. Néanmoins, cette réglementation est un progrès dans la réglementation du domaine de la conservation des données et peut être une source d'inspiration pour trouver des solutions en vue de respecter pleinement les droits de l'homme.

Le 30 décembre 2016, une nouvelle loi est entrée en vigueur au Royaume-Uni, réglementant notamment la question de la conservation des données[55]. En vertu de la nouvelle loi, le secrétaire d'État peut ordonner aux fournisseurs de services de ne conserver les informations nécessaires sur les communications électroniques que si cette conservation est nécessaire et proportionnée et aux fins de la sécurité nationale et de la lutte contre le terrorisme et les infractions pénales graves. Les décisions de conservation peuvent concerner un ou plusieurs fournisseurs de services, tout ou partie des types de données. La période pour laquelle la conservation est demandée ne peut être supérieure à 12 mois à compter du jour de la communication. La loi a fait l'objet de nombreuses et sérieuses critiques, car elle permet toujours de conserver les données de manière indifférenciée, notamment dans l'entourage de la personne, tandis que le secrétaire d'État conserve un large pouvoir discrétionnaire en matière de conservation. La conséquence de cette critique est que le nom «*Snooper's Charter*» a été attribué à la loi.

Selon la disposition nationale belge, les données sont conservées pendant une période pouvant aller jusqu'à six mois pour les besoins des enquêtes et des poursuites visant le terrorisme et les infractions pénales graves. L'accès est impossible sans une ordonnance du tribunal. Cette approche ne résout pas le problème de la non-sélectivité.

Au mois de décembre 2017, en Italie, une loi est entrée en vigueur obligeant les fournisseurs de services à conserver les données des communications électroniques pendant 72 mois, c'est-à-dire 6 ans, à compter de la date de la communication. Bien

[55] Voir: Investigatory Powers Act 2016. Le texte de loi est disponible sur la page web: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

que cette obligation soit considérée comme une exception à l'obligation générale des fournisseurs de services de conserver les données pendant une période comprise entre 12 et 24 mois, dans la mesure où d'ordinaire une période aussi longue est prescrite uniquement aux fins de poursuite de certains crimes, notamment les crimes de terrorisme international, la question qui se pose, néanmoins, est de savoir comment les fournisseurs de services pourraient avoir connaissance des personnes potentiellement liées à la commission de certaines infractions pour déterminer si les données doivent être conservées 72 mois ou de 12 à 24 mois. De plus, la loi italienne ne prévoit pas de mécanisme de conservation ciblée basée sur l'existence d'une relation entre une personne et la planification ou la perpétration d'une infraction pénale[56].

Enfin, il convient de mentionner le travail du groupe de travail du Ministère suédois de la justice chargé de trouver une solution appropriée au nouveau cadre législatif en matière de conservation des données. Le groupe de travail estime qu'il est nécessaire de réviser les règles nationales dans ce domaine, à condition toutefois que cela ne compromette pas l'efficacité de la lutte contre les infractions pénales graves. Il est d'avis qu'il est nécessaire de limiter la conservation des données à ce qui est strictement nécessaire, comme suit: la plupart des données de trafic et de localisation ne seront pas conservées et seules les données nécessaires pour lutter contre les infractions graves devraient être conservées. La conservation des données doit être différente en ce qui concerne la téléphonie et les messages (seules les données sur les communications mobiles seraient concernées tandis que les communications fixes seraient exclues) et internet (conservation des données d'adresse IP et autres données connexes).

Concernant la période de conservation des données, celle-ci varierait en fonction de la catégorie de données. Les données de localisation se conserveraient au maximum deux mois, les données d'internet 10 mois et toutes les autres données pendant 6 mois. L'accès aux données conservées serait limité aux infractions graves et aux personnes soupçonnées de planifier ou de commettre une infraction pénale grave. L'accès serait octroyé sur la base d'une décision antérieure de la juridiction ou d'un organe administratif indépendant. Étant donné que la réglementation nationale suédoise répond à ces exigences, à l'exception de la partie relative à la sécurité nationale, le groupe de travail propose que les procureurs de l'État soient nommés en tant qu'organisme administratifs indépendants pour accorder l'accès aux autorités en charge de la sécurité nationale[57]. Après que le groupe de travail a rédigé son avis, les travaux sur le projet de loi, dont le contenu est actuellement inconnu, sont en cours. Cependant, il est fort à supposer que le groupe de travail a étudié la question de la réduction de la portée des données, ainsi que celle portant sur raccourcissement de la période de conservation des données, sans aborder la question de la restriction du groupe des personnes concernées par la mesure de conservation.

[56] Source: http://www.mmlex.it/the-new-data-retention-provisions-in-italy-from-bad-to-worse/

[57] Source:http://www.regeringen.se/4a8d12/contentassets/b635202b96fc4e4490886e0ef8601e66/datalagring--brottsbekampning-och-integritet-sou-201775; pp. 34-45

Lorsque l'on analyse attentivement les arrêts de la Cour de justice de l'Union européenne, on peut affirmer que les États membres auront beaucoup de difficultés à mettre en œuvre les parties de l'arrêt liées à la conservation, tandis qu'il sera plus facile de trouver une solution législative sur la question de l'accès aux données et des garanties nécessaires contre d'éventuels abus. En effet, concernant le droit d'accès aux données, les États membres pourront limiter cet accès aux personnes qui jouent un rôle essentiel dans la lutte contre le terrorisme et le crime organisé. Il en va de même pour les garanties qui apporteront une protection contre utilisation abusive des données. Mais, en ce qui concerne la conservation, la Cour a demandé qu'elle ne soit pas non-sélective et que c'est précisément cette non-sélectivité qui permet aux autorités compétentes d'intervenir sur les auteurs qui ne sont pas surveillés directement par ces services. La question fondamentale à poser ici est de savoir comment définir un cercle plus restreint de personnes dont les données sont conservées, sans avoir d'impact négatif sur la détection, la prévention et la poursuite du terrorisme et du crime organisé. En outre, la question de la période de conservation des données est très importante, à savoir: quelle est la période minimale à prescrire sans que cela n'affecte le bon déroulement de l'enquête.

Que faire maintenant? Il est essentiel que la Commission européenne communique le plus rapidement possible en proposant des solutions. Ce faisant, elle doit pouvoir apporter des éléments de réponse aux questions soulevées notamment par la Cour européenne: comment garantir la sélection de la conservation des données? Comment s'assurer que l'accès aux données est limité à ce qui est nécessaire et soumis à une surveillance indépendante? Comment fournir des garanties suffisantes contre l'utilisation abusive des données? Il est également nécessaire d'adopter des réglementations à l'échelle de l'UE pour garantir que les États membres adoptent une approche commune en matière de conservation des données, tout en respectant pleinement les droits des citoyens de l'UE garantis par la Charte. Enfin, à ce stade, la question se pose de savoir quelle approche choisir: rester dans l'attentisme ou adopter une attitude proactive? L'attente de solutions au niveau européen présente l'avantage que la République de Croatie, lorsqu'elle apportera les modifications nécessaires à la législation nationale, aura accès au cadre juridique de la conservation des données pour adapter sa législation nationale. D'un autre côté, le défaut de cette approche réside dans le fait que la législation en vigueur en Croatie, dans l'attente d'une solution européenne, est contraire aux critères établis par la jurisprudence de la Cour de justice de l'Union européenne.

Le fait qu'à ce jour la législation de 17 des 28 États membres de l'UE permettent la conservation des données montre qu'il s'agit d'une question extrêmement importante, complexe et délicate à traiter et que la satisfaction des critères établis par la jurisprudence de la Cour de l'UE constitue un véritable défi. Les États membres sont conscients du rôle crucial et de la contribution de la conservation des données dans la lutte contre le terrorisme et le crime organisé.

La Commission européenne, qui travaille avec les États membres pour résoudre cette question, a déjà annoncé début 2017 l'élaboration de lignes directrices à

l'intention des États membres sur la manière de construire une législation nationale conforme à la pratique de la Cour européenne. Pourtant, aujourd'hui encore, aucune solution n'a été proposée par la Commission européenne. En revanche, la position de la Commission européenne est claire concernant le fait que les autorités répressives devraient avoir accès à une quantité critique de données de communications électroniques. La Commission européenne considère que la législation nationale des États membres de l'UE en matière d'accès aux données a été soumise à des conditions très claires et strictes en matière de respect des droits et libertés fondamentaux et considère que le défi principal réside dans la capacité à trouver des solutions par rapport à la méthode de conservation ciblée des données par les fournisseurs de services.

IX. CONCLUSION

La conservation des données électroniques touche à un domaine multidisciplinaire complexe. Elle couvre non seulement le domaine de la sécurité publique et nationale et du droit de procédure pénale, mais également le domaine du respect des droits de l'homme et des libertés fondamentales. Comme il est nécessaire de garantir la sécurité de tous les citoyens de l'UE mais aussi le respect de leur vie privée, il est nécessaire de trouver le juste équilibre entre les intérêts publics et privés. Les droits de l'homme ne bénéficient pas d'une protection illimitée, mais toute restriction des droits et libertés ne peut être justifiée que si elle est nécessaire et correspond aux objectifs d'intérêt général. Il est indéniable à cet égard que la lutte contre les infractions pénales graves, la criminalité organisée et le terrorisme est d'une importance capitale pour la protection de la sécurité publique et qu'elle est donc dans l'intérêt général. Mais cela ne signifie pas que toute mesure concrète est justifiée et nécessaire pour réaliser ces intérêts légitimes. Pour justifier une ingérence, la restriction imposée doit être proportionnelle à l'objectif recherché. Or, la réglementation de la conservation des données au niveau de l'Union européenne est fragmentée et une approche commune est nécessaire pour éliminer le vide juridique résultant de l'invalidation de la Directive sur la conservation des données. L'instrument législatif devrait fixer des normes communes minimales pour tous les États membres de l'UE et garantir la vie privée des citoyens de l'UE tout en garantissant la protection contre le terrorisme et les infractions pénales graves.

Parmi les questions soulevées par la Cour de justice dans le domaine de la conservation, l'accès et la prévention de l'utilisation abusive des données conservées, la question la plus complexe est celle de la réglementation concernant la conservation des données tandis qu'il parait moins délicat de trouver une solution acceptable concernant l'accès aux données et les garanties de protection contre l'utilisation abusive de celles-ci. A ce sujet, deux problèmes sont mentionnés : la question de la sélectivité de la conservation des données relatives aux utilisateurs des télécommunications et la question des périodes de conservation. Celle-ci fait essentiellement référence à la question de la période minimum nécessaire pour

la conservation, sans nuire à l'efficacité de la prévention, de la détection et de la poursuite d'infractions pénales graves. En ce qui concerne le groupe de personnes dont les données doivent être conservées, il n'y a pas de réponse claire. L'autorité répressive estime nécessaire de conserver les données de tous les utilisateurs de communications électroniques et de toutes les personnes physiques ainsi que de la plupart des personnes morales sans qu'au moins un lien indirect avec une activité criminelle grave ne soit nécessairement mis en évidence. Pour la détermination sélective du groupe de personnes dont les données seront conservées, il est fondamental que les autorités compétentes des États membres disposent d'une solide capacité d'évaluation des risques et déterminent, sur la base de ces estimations, le groupe de personnes dont les données doivent être conservées. Dans ce cadre, il faut être conscient qu'il n'existe pas d'évaluation des risques suffisamment fiable permettant d'affirmer qu'aucun individu n'a pu la contourner. La question est donc de savoir si l'on est prêt à prendre ce risque pour préserver les droits fondamentaux. En outre, la pratique montre que les autorités répressives n'utilisent pas les données conservées seulement pour la détection et la poursuite du terrorisme et du crime organisé, mais également dans des cas tels que la disparition d'enfants. Ainsi, nous devons garder à l'esprit que si les données étaient conservées de manière sélective, les informations fournies ne seraient plus disponibles pour rechercher les personnes disparues. En ce qui concerne l'accès aux données et la garantie qu'aucun abus ne se produira, il est possible d'améliorer légalement la réglementation, mais aussi de contrôler l'utilisation des données conservées. Le groupe des personnes autorisées devrait être clairement défini et leur droit d'accès devrait dépendre de l'existence d'une autorisation d'un organisme indépendant agréé. Pour conclure, à l'heure actuelle, aucune administration d'un État membre n'a trouvé de réponse à la question clé qui est de savoir comment garantir la sélectivité de la rétention des données, alors que des solutions à d'autres problèmes ont déjà été résolues ou peuvent être résolues par la réglementation existante.

Au sujet des législations nationales régissant la conservation et l'accès aux données, il sera nécessaire de modifier les dispositions en conflit avec la Charte et les sources secondaires du droit de l'UE, en tenant compte des exigences de la jurisprudence de la Cour. Il convient de rappeler que la République de Croatie, en maintenant en vigueur les réglementations nationales qui ne répondent pas aux critères établis par la Cour de justice de l'Union européenne, porte atteinte aux dispositions de la Charte des droits fondamentaux de l'UE et à d'autres sources du droit communautaire relatives à la protection des données personnelles. Par conséquent, des conséquences juridiques liées aux violations du droit européen, y compris des poursuites judiciaires pouvant être engagées contre un État membre par la Commission européenne, ainsi que des recours individuels devant les juridictions nationales pour obtenir une indemnisation, sont possibles[58].

[58] Goldner Lang I., Perišin T, S. Vasiljević, Mataija M., Carević M., Kuhta F (2014); Avis juridique des membres du Département européen de droit public de la Faculté de droit de l'Université de Zagreb sur les conséquences juridiques de l'arrêt de la Cour de l'Union européenne dans les affaires jointes C-293/12 et C-594/12 en République de Croatie; p. 8-9.

L'arrêt *Tele2* a été adopté il y a moins de deux ans. Depuis lors, de nombreuses discussions ont été menées au niveau de l›UE comme au niveau des États membres. A ce jour, elles n'ont toujours pas abouti à des propositions législatives concrètes qui respecteraient de manière adéquate les vues de la Cour sur la conservation des données. Certains États membres ont décidé d'attendre la proposition de la Commission européenne concernant la future réglementation du domaine de la conservation des données pour conformer leur réglementation nationale. En attendant, les réglementations nationales en vigueur continuent d'affecter la vie privée des individus en portant atteinte à leurs droits. C'est la raison pour laquelle tous les États Membres devraient redoubler d'efforts pour mettre en place rapidement des dispositions juridiques conformes aux respects des droits fondamentaux permettant de conserver les données sans outrepasser ce qui est strictement nécessaire à la lutte contre le crime organisé et le terrorisme.

ABSTRACT

The data retention regulatory framework has been one of the most pressing issues in the European Union for a last few years. Main challenge for EU and its Member States was to strike a balance between security requirements, by taking measures against terrorism and organized crime, and ensuring the protection of human rights and fundamental freedoms. Following the terrorist attacks in the United States and Europe at the beginning of the last decade, the need for introducing the obligation to collect and retain electronic communications data has been identified for the purpose of more effective suppression of terrorism and serious criminal offenses. Legislative initiatives at EU level have resulted in the adoption of regulations setting out a framework for data retention. It is indisputable that data retention is a very useful and effective mean for preventing, detecting, investigating and prosecuting criminal offenses. But at the same time it represents an extremely "invasive" interference in the fundamental rights and freedoms. In particular, the right to privacy and the right to freedom of expression, guaranteed by the Charter of Fundamental Rights. The European Court of Justice in its judgments Digital Rights and Tele2 pointed out a violation of fundamental rights in EU and Member States data retention legislation. The text analyses the scope and impact of the judgments in question on the national legislation and analyses the key human rights standards regarding data retention that the European Court of Justice has pointed out in its decisions. After the ECJ judgment, EU member states, including the Republic of Croatia, have faced a major challenge in improving the legal framework for data retention. In this respect, an analysis of the relevant domestic legal framework is provided, as well as the need to review certain solutions for the purpose of full compliance with the requirements and criteria set by the ECJ.

Key words: *EU, acquis, Data retention, European Court of Justice, Data Retention Directive, Traffic Data, Secrecy of Communications, Security, Terrorism, Privacy, Personal Data Protection*