La directive sur la conservation des données, son invalidation et les obligations de la Belgique

Félix GUILLAUME
Stagiaire juriste LDH

Introduction

1. Imaginez la situation suivante : vous êtes dans la salle d'attente de votre médecin et vous téléphonez à votre conseiller conjugal, ou vous envoyez un sms à un journaliste, ou vous écrivez un courriel à votre avocat. Voici une esquisse de ce que les autorités nationales et les sociétés de télécommunications savent et sauront de vous, pendant douze à trente-six mois : vos nom, prénom et adresse ; la date et le lieu de souscription de votre abonnement ; la date et l'heure de l'activation de votre abonnement ; la façon dont vous payez votre abonnement, ainsi que la date à laquelle le paiement est effectué ; votre numéro de téléphone ; le fait que vous communiquez avec un conseiller conjugal, un journaliste ou un avocat ; la date et l'heure exacte du début et de la fin de votre appel ; le fait que vous vous trouvez chez un médecin (art.4 de l'arrêté royal d'exécution du 19 septembre 2013).

2. La rétention de cette multiplicité de données trouve son origine dans la directive 2006/24/CE (I), transposée en Belgique par une loi et un arrêté royal (II). Récemment, le 8 avril 2014, la Cour de justice de l'Union européenne a eu à se pencher sur la question de la validité de la directive, en confrontant cette dernière au respect du droit à la vie privée. C'est dans ce cadre que la Cour a conclu à l'invalidité de la directive (III). Il y a dès lors lieu de voir quelles sont les conséquences d'un tel arrêt sur les normes nationales adoptées en Belgique, en vue de la transposition de la directive européenne (IV). En sus d'ébranler la vie privée, le mécanisme de rétention des données érigé par la directive et les normes nationales est à même de porter atteinte à d'autres droits fondamentaux concernant chacun d'entre nous (V).

I. La directive européenne et son état actuel

3. La directive 2006/24/CE a été adoptée par le Parlement européen et le Conseil le 15 mars 2006[i]. Son objectif était d'harmoniser les dispositions des Etats membres relatives aux obligations de conserver certaines données (ou « métadonnées ») générées ou traitées par les fournisseurs de services de communications électroniques (art.1er, §1er dir.). Devaient ainsi être conservées, pour une durée allant de six mois à deux ans, de multiples données, telles que les numéros de téléphone appelés depuis un téléphone mobile, la localisation géographique de l'émission de l'appel, la date, l'heure et la durée des communications, etc., sans toutefois que le contenu de ces dernières ne soit traité (art.5 et 6 dir.).

4. Les données conservées devaient être utilisées à des fins de recherche, de détection et de poursuite d'infractions graves (art.1er, §1er dir.). En effet, c'est marquées par les attentats terroristes de Madrid et de Londres (respectivement de 2004 et de 2005) que les institutions de l'Union européenne ont adopté la directive[ii].

5. Par son arrêt du 8 avril 2014 (arrêt des affaires jointes C-293/12 et C-594/12)[iii], que nous étudierons plus en profondeur *infra* (partie III), la Cour de justice de l'Union européenne a déclaré la directive invalide. Nous verrons plus loin les conséquences directes de cet arrêt sur la directive elle-même (voir *infra*, pt.27).

II. La loi et l'arrêté royal belges de transposition

6. Lorsque l'Union européenne adopte une directive, les Etats membres ont l'obligation de la transposer par une mesure nationale d'exécution, au risque de se faire condamner en manquement pour défaut de transposition. Grâce à une déclaration concernant la directive, la Belgique a différé la date maximale de transposition, initialement le 15 septembre 2007, au 15 mars 2009 (comme cela est autorisé par l'art.15, §3 dir.). Malgré cette période supplémentaire, ce n'est qu'en 2013 que la Belgique a adopté les mesures nationales nécessaires : la loi du 30 juillet 2013[iv] et l'arrêté royal d'exécution du 19 septembre 2013[v].

7. L'une et l'autre sont en apparence assez fidèles à la directive. La disposition centrale de la loi est son art.5, qui modifie l'art.126 de la loi du 13 juin 2005 et prévoit, comme l'impose la directive, une obligation de conservation de certaines données aux fournisseurs de services de communications électroniques. Les données concernées sont énumérées dans l'arrêté royal. La loi fixe une durée de conservation de douze mois, qui peut se voir prolongée de six mois, voire de douze autres mois ou au-delà[vi], par arrêté royal, dans des situations où la sécurité publique, la santé publique, l'ordre public ou la défense du Royaume l'exigent. Une procédure spécifique est prévue, dans ce dernier cas de figure, et implique un avis de la Commission vie privée, dont l'objectif est de « *veille*[r] *à ce que les données à caractère personnel soient utilisées et sécurisées soigneusement* »[vii]. Si ce dernier élément de procédure semble assurer l'application, dans une certaine mesure, du droit au respect de la vie privée, il faut tout de même relever qu'il ne s'agit que d'un avis, qui ne doit dès lors pas obligatoirement être suivi dans le processus de prise de décision de prolongation. Il est également à noter que la Commission vie privée intervient alors que les données sont *déjà* conservées depuis près d'un an et qu'elle n'est pas impliquée dans le mécanisme de conservation dès l'amorce de celui-ci.

8. Certaines digressions à la directive peuvent toutefois être constatées dans la loi de transposition. D'abord, alors que la directive exclut de son champ d'application le contenu des communications électroniques, la loi nationale n'écarte pas ce contenu de manière aussi absolue. En effet, en ce qu'elle ajoute les termes « *sauf disposition légale contraire* », il y a lieu de considérer qu'elle permet au législateur une échappatoire sur laquelle ce dernier pourra se baser pour prendre une disposition autorisant l'Etat belge à conserver des données révélant le contenu des communications (art.126, §1er, al.5 de la loi du 13 juin 2005[viii]). À nos yeux, une telle possibilité – et rien que l'existence même de la possibilité – donne au mécanisme de conservation une ampleur qui dépasse démesurément le mandat de la directive et serait à même de renverser – encore plus que ce qu'ils sont déjà – le droit

au respect de la vie privée, le secret des sources, le secret professionnel, etc., comme nous le verrons *infra*.

9. Egalement, la finalité de la directive et celle de la loi divergent. Comme nous l'avons précisé *supra* (pt.4), la finalité de la directive est de lutter contre les infractions *graves*, concept flou, confus, qui fixe néanmoins un certain seuil d'intensité de l'infraction. Ce dernier seuil est écarté par la loi de transposition, qui stipule que les données sont conservées en vue de lutter contre les crimes et délits de droit commun, ce qui est bien moins restrictif et étend l'objectif du mécanisme de conservation mis en place (même si la directive précise que les infractions graves doivent être définies dans le droit interne des Etats membres : art.1er, §1er dir.).

10. A l'heure actuelle, tant la loi de transposition que l'arrêté royal existent toujours dans l'ordre juridique belge. Cependant, à l'image de ce qui a été fait en Roumanie, en Allemagne, en Bulgarie, à Chypre, ou encore en République Tchèque[ix], la Liga voor Mensenrechten et la Ligue des droits de l'Homme ont introduit, le 23 février 2014, un recours en annulation contre la loi devant la Cour constitutionnelle belge, afin de la voir disparaitre.

III. L'arrêt de la Cour de justice de l'Union européenne

A. Le contexte de l'arrêt

11. Dans son arrêt du 8 avril 2014, la Cour de justice conclut à l'invalidité de la directive sur la conservation des données. Il s'agit d'un arrêt rendu pour deux affaires jointes, c'est-à-dire que deux recours distincts devant la Cour ont été rassemblés, du fait de leur connexité, pour que la Cour n'y réponde qu'en un seul et même arrêt.

12. La Cour répond aux questions préjudicielles en validité posées par deux juridictions suprêmes – la *High Court* irlandaise et la *Verfassungsgerichtshof* autrichienne – qui voyaient devant elles introduits des recours portant sur la légalité des lois de transposition de la directive sur la conservation des données. Dans une telle situation, les juridictions nationales ne s'estiment « *pas en mesure de trancher les questions relatives au droit national dont* [elles sont saisies] *sans que la validité de la directive 2006/24 ait été examinée* » (arrêt, §18) et ont dès lors l'obligation, en tant que juridictions suprêmes, de poser une question préjudicielle en validité des actes pris par les institutions de l'Union à la Cour de justice de l'Union (art.267, al.3 TFUE). On se trouve donc dans un schéma dans lequel les juridictions nationales suspendent provisoirement les recours introduits devant eux, dans l'attente d'une réponse apportée par la Cour de justice (arrêt, §§18 et 21).

B. La question centrale de l'arrêt

13. En l'espèce, la question posée par les deux juridictions nationales de renvoi était, en substance, identique : il s'agissait pour la Cour « *d'examiner la validité de la directive 2006/24 à la lumière des articles 7, 8 et 11 de la Charte* [des droits fondamentaux[x]] » (arrêt, §22). Ces articles traitent respectivement du respect de la vie privée et familiale, de la protection des données à caractère personnel et de la liberté d'expression et d'information.

14. La conception de la vie privée, bien que consacrée dans de multiples dispositions, qu'elles soient internationales ou nationales, constitutionnelles ou législatives, ne revêt aucune définition juridique. C'est là l'une des principales difficultés, puisque de la détermination de ce que recoupe la vie privée dépendront les droits qui y sont relatifs. La doctrine s'est d'innombrables fois penchée sur la notion, dont nous retenons la suivante analyse d'O. DE SCHUTTER :« *Le concept de vie privée rassemble trois composantes, dont la totalité ne se laisse pas enfermer en une définition unique. Le premier aspect est celui de l'intégrité physique de l'individu* [...]. *Le deuxième aspect est celui de la confidentialité de certaines informations à caractère personnel, dont l'individu peut refuser la révélation publique* […]. *Enfin, un troisième aspect du concept de vie privée émerge lorsqu'on affirme* […] *son droit à un libre épanouissement de sa personnalité : lorsque sa vie privée est considérée sous cet angle, l'individu est*

considéré non pas isolément, mais dans les relations qu'il noue avec autrui, et à travers lesquelles il se développe en retour »[xi].
Nous verrons que ce sont les deuxième et troisième aspects qui sont ici concernés.

15. Etant donné qu'avec le Traité de Lisbonne (2009), la Charte « *s'est vue confier la même force juridique obligatoire que les traités* »[xii] (art.6, §1er TFUE), devenant ainsi du droit primaire, la question fondamentale posée ici est de vérifier si la directive – instrument juridique de droit dérivé – respecte la Charte, qui lui est supérieure.

C. Le raisonnement de la Cour

16. La Cour apporte une réponse à la question de manière très structurée, chaque étape étant conditionnée par la précédente. Elle examine d'abord si la vie privée et les données à caractère personnel sont concernées par la directive (a). Elle procède ensuite à l'examen de l'existence d'une ingérence dans les droits invoqués (b). Elle vérifie enfin si l'ingérence est justifiée (c).

17. (a) La Cour souligne en un premier temps que les données récoltées, « *prises dans leur ensemble, sont susceptible de permettre de tirer des conclusions très précises concernant la vie privée* » (arrêt, §27) et que la conservation des données « *constitue un traitement des données à caractère personnel* [...] *et doit, ainsi, nécessairement satisfaire aux exigences de protection des données* » (arrêt, §29). Il est donc pertinent de se poser la question du respect de la vie privée (art.7 Charte) et de la protection des données à caractère personnel (art.8 Charte) dans le cadre du litige dont est saisie la Cour.

18. (b) Dès lors, il y a lieu d'établir s'il y a une ingérence dans les droits consacrés aux articles 7 et 8 de la Charte. En ce que la directive impose une obligation de conservation de données relatives à la vie privée, prévoit le traitement de ces dernières et autorise l'accès à ces données aux autorités nationales, la Cour conclut, de manière satisfaisante, que l'ingérence est « *d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave* » (arrêt, §37). Elle relève également que le mécanisme mis en place par la directive « *est susceptible de générer dans l'esprit des* [utilisateurs de services de communications électroniques] *le sentiment que leur vie privée fait l'objet d'une surveillance constante* » (arrêt, §37).

19. (c) Etant donné que les droits ébranlés ne sont pas absolus et sont dès lors susceptibles de dérogation, la Cour vérifie si l'ingérence constatée est justifiée. Certaines conditions doivent à cet égard être respectées, conformément à l'article 52, §1er de la Charte (arrêt, §38) :

- l'ingérence doit être prévue par la loi ;
- respecter le contenu essentiel des droits et libertés garantis par la Charte ;
- dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui (i) et qu'elles sont nécessaires (ii).

20. Concernant la première condition, il n'y a aucun doute, en l'espèce, que l'ingérence est prévue par la loi. De même, la deuxième est remplie, étant donné que la directive « *ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel* » et que « *certains principes de protection et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques* » (arrêt, §§39 et 40).

21. (i) Quant à l'objectif d'intérêt général poursuivi par la directive, la Cour rappelle l'article 1er, §1er de cette dernière (exposé *supra*, pt.4), qui dispose que l'objectif matériel de la directive est « *de contribuer à la lutte contre la criminalité grave et, ainsi, en fin de compte, à la sécurité publique* » (arrêt, §41). La Cour affirme qu'il s'agit bien d'un objectif d'intérêt général poursuivi par l'Union et que, plus est, les données collectées sont un instrument utile à la poursuite de cet objectif (arrêt, §§42-44).

22. (ii.1) Quant à la nécessité, la Cour précise que « *le principe de proportionnalité exige* [...] *que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs* » (arrêt, §46). En l'espèce, la Cour souligne qu'elle procédera à un contrôle strict de proportionnalité, étant donné la gravité de l'ingérence (comme relevé au pt.15) et l'importance des droits en jeu (arrêt, §48).

23. (ii.2) Cette intransigeance dans l'analyse de la Cour se voit dans l'exigence d'un cadre rigoureux, de règles claires et précises et de garanties suffisantes dans le mécanisme mis en place par la directive (arrêt, §54). La Cour va d'abord constater l'absence générale de limites dans la directive. Est ainsi visée la « *quasi-totalité de la population européenne* [...]*, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales* » (arrêt, §§56 et 58). Sont ainsi également visées les personnes qui n'ont aucun lien avec des infractions graves, voire même des personnes soumises au secret professionnel, ce que la Cour ne manque pas de remarquer (arrêt, §58).

24. (ii.3) De plus, le manque de critère objectif, de conditions matérielles et procédurales, ainsi que de contrôle juridictionnel préalable pour déterminer l'accès des autorités nationales aux données conservées est également vu comme un manque de limites au mécanisme mis en place (arrêt, §§60-62). Par ailleurs, aucun critère ne permet de limiter la durée de la conservation au strict nécessaire (arrêt, §§63-64). Enfin, le manque de garanties suffisantes concernant la sécurité et la protection des données conservées et l'absence d'obligation que les données en cause soient conservées sur le territoire de l'Union pose problème, notamment du fait que cela empêche un contrôle par une autorité indépendante sur le territoire de l'Union (arrêt, §§66-68).

25. (ii.4) La Cour en déduit donc que la directive « *ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux* » et que, non seulement l'ingérence est d'une gravité particulière, mais elle manque de surcroît d'encadrement permettant de garantir que le mécanisme est effectivement limité au strict nécessaire (arrêt, §65).

26. En conclusion, la Cour vient à dire que le législateur de l'Union a, en adoptant la directive 2006/24, excédé les limites qu'impose le respect du principe de proportionnalité, au regard des articles 7 (respect de la vie privée), 8 (protection des données à caractère personnel) et 52, §1er (limitation de l'exercice des droits et libertés fondamentaux) de la Charte (arrêt, §69).

D. La conclusion de la Cour et les effets de l'arrêt dans l'ordre juridique européen et pour les juridictions de renvoi

27. La Cour déclare que la directive 2006/24 est invalide (arrêt, §71), ce qui a une influence dans l'ordre juridique de l'Union. L'application par analogie de l'article 266 TFUE a pour conséquence que « *plus personne ne peut appliquer l'acte déclaré invalide et* [que] *l'autorité auteur de l'acte doit faire disparaître l'illégalité* »[xiii] en prenant les mesures nécessaires à l'exécution de l'arrêt préjudiciel en validité[xiv]. Dans le cas ici analysé, il revient à la Commission d'apporter des modifications à la directive, prenant en compte les points cernés par la Cour comme étant litigieux. De plus, n'étant pas limité dans le temps, l'arrêt revêt un effet *ex tunc*, c'est-à-dire avec effet rétroactif. Par conséquent, « *la déclaration d'invalidité prend effet à la date de l'entrée en vigueur de la directive* »[xv].

28. En outre, l'arrêt est obligatoire pour les juridictions de renvoi – la *High Court* irlandaise et la *Verfassungsgerichtshof* autrichienne – qui devront prendre en compte la conclusion de la Cour, à savoir l'invalidité de la directive, dans le cadre de leur propre décision nationale. Pour ce qui est du présent cas, les mesures nationales de transposition de la directive étaient contestées devant les juridictions nationales. Le recours préjudiciel en validité s'inscrit dans un schéma en chaîne : une loi nationale a été adoptée en vue de transposer une directive européenne. Cependant, celle-ci est incompatible avec une norme supérieure de droit européen, ce qui entraîne son invalidité. La question reste donc de savoir quel effet cette invalidation de la directive a sur la validité des mesures nationales de transposition. Etant donné que la base de ces mesures nationales, la directive, est

illégale, il y a lieu, pour les juridictions nationales, de conclure à l'illégalité de ces mesures de transposition.

IV. Les effets de l'arrêt dans l'ordre juridique belge

29. Deux effets de l'arrêt dans l'ordre juridique belge peuvent être définis. Le premier touche au comportement des autorités nationales vis-à-vis de la loi (A), alors que le second concerne les juridictions qui seraient amenées à se poser des questions relatives à la directive invalidée (B).

A. Les autorités nationales belges

30. Les effets de l'arrêt ne se limitent pas aux seules juridictions de renvoi et aux institutions européennes. Dans l'affaire *Fratelli Martini*, la Cour a affirmé que, « [*s*]*'agissant des autorités nationales,* [...] *il appartient en premier lieu à celles-ci de tirer les conséquences dans leur ordre juridique d'une déclaration d'invalidité* »[xvi]. Dès lors, les autorités nationales doivent, d'elles-mêmes, revoir leur loi nationale, en cas de déclaration d'invalidité du socle qui sert de base à celle-ci, à savoir la directive. Dans le cas soumis à notre étude, ces deux normes nationales doivent être revues par les autorités nationales belges, puisqu'elles sont le fruit d'un arbre malade : ces actes sont arrêtés « *en vue de donner exécution à des actes non valides émanant des institutions communautaires* »[xvii]. D'autant plus que la loi et l'arrêté royal fixent des règles plus larges et attentatoires que les dispositions de la directive.

31. C'est donc parce que l'on se situe dans une relation de cause – la directive – à effet – les mesures de transposition belges – que le gouvernement belge doit lui-même prendre l'initiative de reconsidérer celles-ci, sans l'intervention d'aucun autre acteur. Au-delà de la simple reconsidération, il y a lieu pour le gouvernement belge de supprimer la loi et l'arrêté royal de l'arsenal législatif belge[xviii].

32. Il est important de préciser que l'effet de l'arrêt ne doit toutefois pas être surestimé : il s'agit ici d'une victoire concernant la directive seule et non concernant la politique même de conservation de données. Les Etats membres – de même que l'Union européenne – gardent donc la possibilité de construire un nouveau mécanisme de conservation de données qui prendrait en compte les raisons pour lesquelles la directive s'est vue invalidée[xix]. Cependant, comme nous l'exposons ci-dessous (pts.35 et 36), il y a lieu de constater que la législation belge n'est pas conforme aux points soulevés par la Cour, de telle sorte que la Belgique ne peut poursuivre sa politique de conservation de données telle qu'elle existe en son état actuel.

B. Les juridictions nationales belges

33. Il est malheureux de constater qu'en dépit des obligations qui pèsent sur les épaules du gouvernement, celui-ci n'a pas encore agi, au sujet de la loi du 30 juillet 2013 et l'arrêté royal d'exécution du 19 septembre 2013. L'occasion est malgré tout offerte à la Cour constitutionnelle de forcer le passage, puisqu'un recours en annulation contre la loi a été introduit devant la Cour constitutionnelle. Il faut d'emblée noter que, même si le recours est antérieur à l'arrêt de la Cour de justice, la Cour constitutionnelle devra tout de même tenir compte de celui-ci.

34. Bien plus qu'une occasion, il s'agit même pour la Cour constitutionnelle d'une obligation, étant donné que l'arrêt de la Cour de justice a un effet *erga omnes*, ce qui signifie que « *l'arrêt de la Cour est* [...] *obligatoire pour tout autre juge* [que les juges de renvoi] »[xx]. En effet, suite à une déclaration d'invalidité d'un acte européen par la Cour de justice, dans le cadre d'un recours préjudiciel en validité – ce qui est le cas de notre affaire –, « *tout autre juge* [national doit] *considérer cet acte* [européen] *comme non valide pour les besoins d'une décision qu'il doit rendre* »[xxi]. La métaphore de l'arbre malade du pt.30 peut donc être reprise.

35. Outre les obligations qui incombent à la Cour constitutionnelle en vertu du droit européen[xxii], une analogie peut être faite entre la directive 2006/24/CE et la loi du 30 juillet 2013 – et principalement au niveau du contrôle de proportionnalité –, de telle manière que la Cour de justice a déjà

« prémâché » le travail de la Cour constitutionnelle. En effet, les points retenus par la Cour de justice lors de son analyse de la directive 2006/24/CE se retrouvent dans la loi du 30 juillet 2013[xxiii] :

- Tout comme la directive, la loi ne fait aucune différenciation, au sein des personnes et des moyens de communication électronique visés, en fonction de l'objectif de lutte contre les crimes et délits (arrêt, §57 ; voir pt.23 *supra*). Pour reprendre les mots de la Cour, la *quasi-totalité de la population belge*, dont des personnes soumises au secret professionnel, est dès lors épiée (arrêt, §56) ;

- La loi ne prévoit pas non plus de critère objectif, permettant de limiter l'accès des autorités aux données conservées, de telle sorte qu'aucune « *protection efficace des données contre les risques d'abus ainsi que contre l'accès et l'utilisation (illicites) des données* »[xxiv] n'est assurée (arrêt, §62 ; voir pt.24 *supra*) ;

- Comme il l'est relevé au pt.7 (ainsi qu'à la note vi) de cette étude, le Roi a la possibilité de prolonger la durée de conservation des données jusqu'à un délai outrepassant les vingt-quatre mois maximum fixés par la directive. Outre le fait que la loi viole le prescrit de la directive, elle ne prévoit pas non plus de critère qui détermine clairement la durée de la conservation, dans cet intervalle de temps (arrêt, §64 ; voir pt.24 *supra*) ;

- Enfin, la loi ne garantit pas qu'un contrôle puisse être exercé facilement sur les organismes de conservation des données par une autorité indépendante nationale, en ce qu'elle n'impose pas que les données en cause soient conservées sur le territoire belge, « *ni même sur le territoire de l'Union européenne* »[xxv] (arrêt, §68 ; voir pt.24 *supra*).

36. Au vu de ce qui précède, en employant le raisonnement et les critères suivis par la Cour de justice, il semble clair que la loi ne répond pas aux exigences de clarté et de précision requis dans le cadre de la justification de l'ingérence dans, par ailleurs, le droit au respect de la vie privée. La Cour constitutionnelle a donc à sa disposition un canevas qui l'aiderait à conclure à l'annulation de la loi du 30 juillet 2013.

V. Réflexions

37. Il s'agit ici d'apporter des observations supplémentaires sur différentes questions, outre celle de la vie privée, que suscite le mécanisme mis en place par la directive européenne et les normes nationales[xxvi].

A. La liberté d'expression

38. Dans son arrêt, la Cour se concentre sur le droit au respect de la vie privée et à la protection des données à caractère personnel et, par économie de procédure, ne s'attarde pas à examiner la validité de la directive 2006/24/CE au regard de l'article 11 de la Charte des droits fondamentaux, à savoir le respect de la liberté d'expression (arrêt, §70). Il nous semble cependant capital de relever qu'un tel mécanisme général de conservation de cet ensemble de données constitue une ingérence dans la liberté d'expression. Bien que le contenu des données ne soit pas visé par la directive (rappelons que la loi nationale prévoit une ouverture pour que le contenu puisse être conservé : voir le pt.8), le fait pour un citoyen de savoir que l'ensemble de ses communications sont tracées a sans aucun doute un impact sur sa fréquence d'appels, d'envoi de courriers électroniques, etc. En effet, il se refuserait de s'adresser librement à des journalistes, partis politiques, ou encore des organisations religieuses, spirituelles, philosophiques, etc., sachant que les autorités publiques auront connaissance de ses flux de communication avec ceux-ci. La liberté d'expression du citoyen se retrouve donc affaiblie.

39. De plus, le comportement de la personne à la source de la communication a un impact sur celui du destinataire, puisque certaines données de celui-ci, comme son nom et son adresse, sont conservées de telle manière que tant son droit à la vie privée que sa liberté d'expression (il refuserait que l'on communique avec lui) sont incidemment touchés par le mécanisme de conservation.

40. Notons tout de même qu'au §25 de l'arrêt, la Cour souligne que la directive soulève des questions relatives au respect de la liberté d'expression, mais sans aller plus en profondeur et sans constater qu'il y a ingérence dans celle-ci.

B. La liberté de circulation et la liberté de réunion et d'association

41. De la même manière, dès lors que le lieu de l'émission d'un appel est conservé (art.5, f) dir. et art.3, §2, 2° et 4, §2, 6° de l'AR du 19 septembre 2013), la liberté de circulation des citoyens s'en trouve altérée. Le citoyen éprouverait en effet moins l'envie de se déplacer, sachant que les autorités seraient à même de connaître les lieux où il se trouve et auxquels il se rend : chez le médecin, au siège d'un parti politique, dans un établissement religieux, etc. et dont elles pourraient tirer certaines conclusions (la question de savoir si ces conclusions sont hâtives ou pas relève d'un autre débat...).

42. Ce raisonnement s'applique aussi à la problématique de la liberté de réunion et d'association : ce mécanisme de conservation des données, en ce qu'il permet aux autorités d'avoir connaissance des destinataires des communications et du lieu des émissions de celles-ci, constitue un frein pour le citoyen désireux de s'investir dans une vie associative, syndicale, etc.

C. Le secret professionnel et le secret des sources

43. La loi belge viole également le secret professionnel et le secret des sources, étant donné que les autorités ont connaissance des noms des patients des médecins et des psychologues, celui des clients des avocats et des conseillers conjugaux, celui des sources des journalistes, celui des fidèles des ministres du culte, etc. La relation que les citoyens ont avec les personnes tenues au secret professionnel et avec les journalistes est dès lors connue des autorités, ce qui constitue une intrusion, non seulement dans la vie du citoyen, mais également dans le secret auquel ces personnes sont tenues. En effet, les autorités, ainsi que les acteurs commerciaux que sont les compagnies de télécommunications, pourraient dresser une liste des patients des médecins, des clients des avocats, etc., avoir connaissance de la fréquence des communications et ainsi croquer un portrait de plus en plus précis de chacun d'entre nous.

D. Le contenu des communications

44. Cela a déjà été dit (voir *supra*, pt.3), la directive européenne exclut le contenu des communications de son champ d'application. Cependant, nous avons exposé que la loi belge réservait au législateur la possibilité de viser le contenu, en introduisant les termes « *sauf disposition légale contraire* » (voir supra, pt.8). La seconde condition de la justification d'une ingérence, requise à l'article 52, §1er de la Charte, à savoir le respect du contenu essentiel des droits et libertés garantis par la Charte (voir supra, pt.19), n'est dès lors pas respectée par la loi – contrairement à ce que la Cour avait conclu pour la directive – dès lors que la loi *permet de prendre connaissance du contenu des communications électroniques en tant que tel*, pour reprendre les termes de la Cour (voir *supra*, pt.20). La loi ne respecte donc ni le principe de proportionnalité, ni le contenu essentiel des droits garantis par la Charte, ce qui est une lacune substantielle.

E. Les résultats de la directive

45. Certains doutes relatifs à l'efficacité du mécanisme de conservation de données, du point de vue de son objectif – la lutte contre les infractions graves –, peuvent être émis. En 2011, l'Agence fédérale allemande pour la criminalité a publié « *une étude de la police montrant une augmentation des infractions criminelles enregistrées par la police entre 2007 (15.790) et 2009 (16.814). L'utilisation de la conservation des données a permis de solutionner seulement 83,5% des faits contre 84,4% en 2007, sans l'aide de la rétention des données* »[xxvii]. L'utilité du mécanisme et sa capacité à atteindre son objectif sont donc à remettre en question.

Conclusions

46. La directive européenne dont la loi nationale s'est inspirée s'est vue invalidée par la Cour de justice de l'Union européenne, car elle constituait une ingérence particulièrement grave dans le droit au respect de la vie privée, et qu'une telle ingérence ne pouvait être justifiée, à défaut d'être proportionnée.

47. Dans ce cas de figure, les autorités belges doivent, d'elles-mêmes, réagir et conformer la législation nationale à l'arrêt de la Cour, étant donné que celle-ci présente les mêmes défauts de proportionnalité que la directive et ne peut dès lors plus exister en son état actuel. Ce dernier point concernant la proportionnalité est d'ailleurs capital pour la Cour constitutionnelle, saisie d'un recours en annulation contre la loi belge, qui pourra suivre le schéma dressé par la Cour de justice et appliquer celui-ci à la loi nationale. Par ailleurs, du fait de l'effet *erga omnes* de l'arrêt de la Cour de justice, la Cour constitutionnelle doit considérer la directive européenne comme non-valide.

48. Enfin, le mécanisme de rétention de données trouble, outre la vie privée, la liberté d'expression, la liberté de circulation, la liberté de réunion et d'association, le secret professionnel, le secret des sources, ouvre une possibilité d'avoir accès au contenu des communications et n'offre pas les résultats pour lesquels il a été fondé.

Notes

[i] Directive n°2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L.105, 13 avril 2006, pp.54-63, disponible ici.

[ii] X., « Avis de la Cour de justice de l'Union au sujet de la directive sur la conservation des données », *NURPA*, publié le 12 décembre 2013, disponible ici ; cela est révélé dans les considérants (8) et (10) dir.

[iii] C.J.U.E., arrêt du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, affaires jointes C-293/12 et et C-594/12, non encore publié, disponible ici.

[iv] Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle, *M.B.*, 28 août 2013, disponible ici.

[v] Arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 8 octobre 2013, disponible ici.

[vi] Ce point est problématique, du point de vue de la directive, étant donné que celle-ci fixe un délai maximal de conservation de deux ans.

[vii] Accueil du site Internet de la Commission de protection de la vie privée, disponible ici.

[viii] « *Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée.* »

[ix] X. « La directive sur la conservation des données invalidée par la CJUE », *NURPA*, publié le 8 avril 2014, disponible ici.

[x] Charte des droits fondamentaux de l'Union européenne, Parlement européen, Conseil et Commission, faite à Nice, le 7 décembre 2000, *J.O.U.E.*, C83/01, 30 mars 2010.

[xi] O. DE SCHUTTER, « La vidéosurveillance et le droit au respect de la vie privée », *Journal des Procès*, 1996, n°296, p.10.

[xii] X., « Charte des droits fondamentaux », *EUR-Lex*, révisé le 17 juin 2014, disponible ici.

[xiii] M. WATHELET, avec la collaboration de J. WILDEMEERSCH, *Contentieux européen*, 2e édition, Collection de la Faculté de droit de l'Université de Liège, Bruxelles, Larcier, 2014, p.466.

[xiv] C.J.C.E., ordonnance du 8 novembre 1997, *Fratelli Martini*, C-421/06, *Rec.* p.I-152 (pub. somm.), §52, cité par C. NAÔMÉ, *Le renvoi préjudiciel en droit européen, Guide pratique*, 2e édition, Collection JLMB opus, Bruxelles, Larcier, 2010, p.283.

[xv] C.J.U.E., « La Cour de justice déclare la directive sur la conservation des données invalide », Communiqué de presse n°54/14 sur l'arrêt des affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger e.a*., fait à Luxembourg le 8 avril 2014, disponible ici.

[xvi] C.J.C.E., ordonnance du 8 novembre 1997, *Fratelli Martini*, C-421/06, *Rec.* p.I-152 (pub. somm.), §53, cité par C. NAÔMÉ, *op.cit.*, p.283.

[xvii] C.J.C.E., arrêt du 30 octobre 1975, *Rey Soda*, C-23/75, *Rec.* p.1279, disponible ici, §50.

[xviii] M. WATHELET, *op.cit.*, p.465.

[xix] X., « Recommandations du CCBE concernant l'annulation de la directive sur la conservation des données », *CCBE*, 12 septembre 2014, disponible ici, p.3 ; Commission européenne, Memo : « Frequently Asked Questions: The Data Retention Directive », *Commission européenne*, Bruxelles, 8 avril 2014, disponible ici.

[xx] M. WATHELET, *op.cit.*, p.465.

[xxi] C.J.C.E., arrêt du 13 mai 1981, *International Chemical Corporation*, C-66/80, *Rec.* 1981, p.1191, §13, cité par M. WATHELET, *op.cit.*, p.465 et par C. NAÔMÉ, *op.cit.*, p.282.

[xxii] Voir aussi X., « Arrêt de la Cour de Justice de l'Union européenne du 8 avril 2014 », Unité de droit économique, Centre de droit privé de l'ULB, 22 avril 2014, disponible sur ici, pt.4, a, §3.

[xxiii] R. JESPERS, « Les conséquences sur la loi belge du 30 juillet 2013 (rétention de données et l'accès à celles-ci) de l'arrêt de la Cour de Justice de l'Union européenne du 8 avril 2014 », 30 octobre 2014, inédit, p.32.

[xxiv] *Ibid.*, p.34.

[xxv] *Ibid.*, p.36.

[xxvi] Voir X., « Conservation des données : vos moindres faits et gestes sous surveillance », *Stop Data Retention*, disponible ici.

[xxvii] X., « Directive Data Retention: position et enjeux », *Ligue des droits de l'Homme*, disponible ici.