

Décision n° 440
du 8 juillet 2014

concernant l'exception d'inconstitutionnalité des dispositions de la Loi n° 82/2012 sur la conservation de données générées ou traitées par les fournisseurs de réseaux publics de communications électroniques et les fournisseurs de services de communications électroniques accessibles au public, et portant modification et complément de la Loi n° 506/2004 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et de l'article 152 du Code de procédure pénale

publiée au Moniteur officiel de la Roumanie, Partie I, n° 653 du 4 septembre 2014

Résumé :

I. Les motifs de l'exception d'inconstitutionnalité, exception soulevée, d'office, par le Tribunal de Première Instance Constanța – Section pénale, indiquent que la Loi n° 82/2012 est la transposition dans la législation nationale de la Directive 2006/24/CE du Parlement européen et du Conseil de 15 mars 2006 sur la conservation des 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, directive déclarée invalide par l'Arrêt du 8 Avril 2014 de la Cour de Justice de l'Union européenne. On allègue que, par l'arrêt précédemment indiqué, la Cour de Justice de l'Union européenne a jugé que la conservation des données imposée par la Directive 2006/24/CE était susceptible de réaliser l'objectif poursuivi, à savoir la lutte contre la criminalité grave, ainsi que le maintien de la sécurité publique, mais cela impliquait une ingérence importante et particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, sans que cette ingérence fût limitée au strict nécessaire. On fait valoir que tant la solution que les considérations de l'Arrêt du 8 avril 2014 sont aussi applicables dans la présente affaire.

Ainsi, il est indiqué que les dispositions de l'article 152 du Code de procédure pénale et de la Loi n° 82/2012 apparaissent comme étant inconstitutionnelles, en violation des dispositions de l'article 26 de la Constitution. À cet égard, il est fait valoir que la Loi n° 82/2012 n'incrimine que l'accès intentionnel, l'altération ou le transfert, sans autorisation, des données retenues selon les dispositions de cette loi, sans offrir une protection efficace des données contre les risques d'abus ou d'utilisations illégales. Il convient également de noter que la même loi impose la conservation des données pour une période de 6 mois, sans distinguer entre les catégories de données, en fonction des personnes concernées ou de leur utilisation éventuelle par rapport à l'objectif poursuivi et qu'aucun critère objectif n'est prévu pour déterminer la durée de la conservation, pour la limiter au stricte nécessaire. On invoque en outre que, à l'instar de la Directive 2006/24/CE, la Loi n° 82/2012 ne prévoit pas l'obligation de conserver les données sur le territoire de l'Union européenne, sans que le contrôle du respect des exigences en matière de protection et de sécurité par une autorité indépendante soit pleinement garanti, ce qui est contraire à la Charte des droits fondamentaux de l'Union européenne, un tel contrôle étant un élément essentiel de la protection des personnes à l'égard de la gestion des données à caractère personnel.

II. En ce qui concerne ces critiques, la Cour a jugé ce qui suit :

1. La Loi n° 82/2012 sur la conservation de données générées ou traitées par les fournisseurs de réseaux publics de communications électroniques et par les fournisseurs de services de communications électroniques accessibles au public, et portant modification et complément de la Loi n° 506/2004 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques constitue la transposition en droit national de la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE. Toutefois, la Directive 2006/24/CE a été déclarée invalide par l'Arrêt de la Cour de Justice de l'Union européenne du 8 Avril 2014, rendu dans les affaires jointes C 293/12 – *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres* – et C 594/12 – *Kärntner Landesregierung et alii*. Par cet arrêt, l'instance européenne a conclu que la directive analysée était contraire aux dispositions de l'article 7, de l'article 8 et de l'article 52, paragraphe (1) de la Charte des droits fondamentaux de l'Union européenne. La Cour de Justice de l'Union européenne a indiqué, à cet égard, que la Directive 2006/24/CE avait pour principal objectif l'harmonisation des législations des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications de conserver certaines données générées ou traitées, en vue de garantir la disponibilité de ces données pour la prévention, l'investigation, la détection et la poursuite des infractions graves, telles que celles liées à la criminalité organisée et au terrorisme. Il a été constaté, en outre, que la conservation de ces données répondait à un intérêt général, contribuant à la lutte contre la criminalité grave et, partant, à la sécurité publique, et qu'elle ne portait pas atteinte à la substance des droits fondamentaux préservés par la Charte. Toutefois, il a été conclu que les mesures définies par la Directive 2006/24/CE, bien qu'elles ne fussent pas susceptibles d'atteindre l'objectif poursuivi, constituaient une ingérence dans les droits garantis par les articles 7 et 8 de la Charte, qui ne respectaient pas le principe de la proportionnalité entre les mesures prises et l'intérêt général sauvegardé.

2. La Loi n° 82/2012 a été adoptée par le Parlement à la suite du prononcé, par l'instance constitutionnelle, de la Décision n° 1258 du 8 octobre 2009, publiée au Moniteur officiel de la Roumanie, Partie I, n° 798 du 23 novembre 2009, par laquelle il a été constaté que les dispositions de la Loi n° 298/2008 sur la conservation des données générées ou traitées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, et portant modification de la Loi n° 506/2004 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques étaient inconstitutionnelles, la Loi n° 298/2008 constituant la première transposition en droit national de la Directive 2006/24/CE. À cet égard, la Cour a jugé que les garanties légales sur l'utilisation concrète des données retenues – concernant l'exclusion du contenu de la communication ou des informations consultées, comme objet du stockage des données, lors de l'autorisation motivée et préalable du président de l'instance compétente pour juger des faits pour lesquels des poursuites pénales ont été engagées, dans les conditions de l'article 16 de la Loi n° 298/2008 et avec l'application des sanctions visées aux articles 18 et 19 de celle-ci – n'étaient pas suffisantes et appropriées pour éliminer la crainte que les droits personnels, d'ordre intime, étaient violés, de sorte que leur manifestation eût lieu d'une manière acceptable.

3. La loi critiquée, soulevant des problèmes touchant à la protection des droits constitutionnels visés aux articles 26, 28 et 30 de la Loi fondamentale, constitue une intervention législative dans leur champ, motivée par le but même de cette loi, qui est, au niveau national, celui de la Directive 2006/24/CE et consiste de la prévention, la détection et

l'investigation des infractions graves par les organes de poursuites pénales, les instances judiciaires et les organes de l'État avec attributions dans le domaine de la sécurité nationale, objectif pleinement réalisé par la loi soumise au contrôle de constitutionnalité.

4. Tout d'abord, *l'ingérence dans les droits fondamentaux concernant la vie intime, familiale et privée, le secret de la correspondance et la liberté d'expression est d'une grande ampleur et doit être considérée comme particulièrement grave*, et le fait que la conservation des données et leur utilisation subséquente sont faites sans que l'abonné ou l'utilisateur enregistré en soit informé est susceptible d'imprimer dans la conscience des personnes visées le sentiment que leur vie privée fait l'objet d'une surveillance constante.

5. Deuxièmement, les données faisant l'objet de la réglementation, bien qu'ayant un caractère essentiellement technique, sont retenues en vue de fournir les informations sur la personne et sa vie privée. Même si, aux termes de l'article 1, paragraphe (3) de la loi, cela ne s'applique pas au contenu des communications ou des informations consultées lors de l'utilisation d'un réseau de communications électroniques, les autres données conservées, ayant comme but l'identification de l'appelant et de l'appelé, c'est-à-dire de l'utilisateur et du destinataire d'une information communiquée par voie électronique, de la source, de la destination, de la date, de l'heure et de la durée d'une communication, du type de communication, de l'équipement de communication ou des dispositifs utilisés par l'utilisateur, de la localisation de l'équipement de communications mobiles, ainsi que d'autres « données requises » - non définies par la loi -, sont susceptibles de porter atteinte à la manifestation libre du droit à la communication ou d'expression. En particulier, les données eues en vue aboutissent à des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, conclusions qui peuvent porter sur les habitudes de la vie quotidienne, les lieux de séjour permanent ou temporaire, les déplacements quotidiens ou d'autres déplacements, les activités déroulées, les relations sociales de ces personnes et les milieux sociaux fréquentés par elles. *Cependant, une telle limitation de l'exercice du droit à la vie intime, familiale et privée et au secret de la correspondance, ainsi que de la liberté d'expression doit avoir lieu d'une manière claire, prévisible et sans ambiguïté, afin d'éliminer, autant que possible, l'éventualité de l'arbitraire ou de l'abus des autorités dans ce domaine.*

6. Troisièmement, *la loi critiquée ne contient pas de règles claires et précises sur le contenu et l'application de la mesure de la conservation et de l'utilisation, de sorte que les personnes dont les données ont été conservées bénéficient de garanties suffisantes pour assurer une protection efficace contre les abus et contre tout accès ou utilisation illicite.* Ainsi, la loi ne prévoit pas de critères objectifs visant à limiter au strict minimum le nombre de personnes qui y ont accès et peuvent ensuite utiliser les données conservées, que l'accès des autorités nationales aux données stockées ne dépend pas, dans tous les cas, du contrôle préalable effectué par une instance ou par une entité administrative indépendante, qui limite cet accès et leur utilisation à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi. Les garanties légales sur l'utilisation concrète des données retenues ne sont pas suffisantes et appropriées pour éliminer la crainte que les droits personnels, d'ordre intime, sont violés, de façon à ce que leur manifestation puisse être effectuée d'une manière acceptable.

7. Outre les arguments avancés ci-dessus, la Cour estime nécessaire, pour une compréhension exacte du mécanisme de la conservation des données, de faire une distinction entre deux étapes différentes. Notant que les données mises en discussion concernent essentiellement les données de trafic et de localisation des personnes, ainsi que les données nécessaires à l'identification d'un abonné ou d'un utilisateur enregistré, le mécanisme régi comporte deux phases, la première étant celle de la conservation et du stockage des données, tandis que la seconde est celle de l'accès à ces données et de leur utilisation.

8. La conservation et le stockage des données qui, normalement, est la première opération du point de vue chronologique, incombe, comme obligation, aux fournisseurs de réseaux publics et de services de communications électroniques accessibles au public. Cette opération est technique, étant menée de façon automatique sur la base de programmes informatiques, pour autant que la loi oblige les fournisseurs désignés par loi de conserver ces données. Considérant que, tant selon la Directive 2006/24/CE que selon la Loi n° 82/2012, la finalité de la conservation et du stockage est générale, de manière à garantir la sécurité nationale, la défense, ainsi que la prévention, l'investigation, la détection et les poursuites pénales des infractions graves, la conservation et le stockage n'étant pas liés et déterminés par un cas concret, il apparaît comme évident le caractère continu de l'obligation des fournisseurs de réseaux publics de communications électroniques et des fournisseurs de services électroniques de conserver ces données pendant toute la période, expressément prévue par le cadre normatif en vigueur, c'est-à-dire sur une période de 6 mois, conformément à la Loi n° 82/2012. En outre, à ce stade, s'agissant exclusivement de la conservation et du stockage d'une masse d'informations, l'identification ou la localisation de ceux qui sont les sujets d'une communication électronique ne se fait pas de manière concrète, cette dernière ne suivant intervenir qu'au cours de la deuxième étape, une fois autorisé l'accès aux données et leur utilisation.

9. La Cour estime que c'est précisément en raison de la nature et de la spécificité de la première phase, dès lors que le législateur estime nécessaire de conserver et stocker les données, que cette opération est la seule qui ne contrevient pas, par elle-même, au droit à la vie intime, familiale et privée, ou au secret de la correspondance. Ni la Constitution ni la jurisprudence de la Cour Constitutionnelle n'interdisent le stockage préventif, sans une certaine occasion des données de trafic et de localisation, à condition toutefois que l'accès à ces données et leur utilisation soient assortis de garanties et respectent le principe de la proportionnalité.

10. Par conséquent, la Cour considère que ce n'est que par rapport à la deuxième phase, celle de l'accès et de l'utilisation de ces données, que se pose la question de la conformité de la réglementation légale avec les dispositions constitutionnelles. En procédant à l'examen les dispositions de la Loi n° 82/2012, sur l'accès des organes judiciaires et des autres organes de l'État avec des attributions dans le domaine de la sécurité nationale aux données stockées, la Cour constate que la loi n'offre pas les garanties nécessaires à la protection du droit à la vie intime, familiale et privée, du secret de la correspondance et de la liberté d'expression des personnes dont les données stockées sont consultées.

11. En effet, tel qu'il a été relevé précédemment, conformément aux dispositions de l'article 1 de la Loi n° 82/2012, les organes de poursuites pénales, les instances judiciaires et les organes de l'État avec attributions dans le domaine de la sécurité nationale ont accès aux données conservées conformément aux dispositions de la présente loi. Toutefois, conformément aux dispositions de l'article 18 de la Loi n° 82/2012, seuls les organes de poursuites pénales sont tenus de respecter les dispositions de l'article 152 du Code de procédure pénale, cette obligation n'étant pas prévue aussi pour les organes de l'État avec des attributions dans le domaine de la sécurité nationale, qui peuvent avoir accès à ces données en vertu des « lois spéciales en la matière », tout comme le prévoit l'article 16, paragraphe (1) de la Loi n° 82/2012. Par conséquent, seule la demande présentée par les organes de poursuites pénales aux fournisseurs de réseaux publics de communications électroniques et aux fournisseurs de services de communications électroniques accessibles au public de transmission des données conservées est soumise à l'autorisation préalable du juge des droits et libertés.

12. Les demandes d'accès aux données conservées en vue de leur utilisation aux fins prévues par la loi, formulées par les organes de l'État avec des attributions dans le domaine de

la sécurité nationale, ne font pas l'objet de l'autorisation ou de l'approbation d'une instance judiciaire, la garantie d'une protection efficace des données conservées contre les risques d'abus, ainsi que contre tout accès et toute utilisation illicites de ces données faisant ainsi défaut. Cette circonstance est susceptible de constituer une ingérence dans les droits fondamentaux à la vie intime, familiale et privée et du secret de la correspondance et, partant, elle est contraire aux dispositions constitutionnelles qui consacrent et protègent ces droits.

13. Sur la base de l'analyse des « lois spéciales en la matière », auxquelles l'article 16, paragraphe (1) de la Loi n° 82/2012 fait référence, la Cour constate que les organes de l'État avec des attributions dans le domaine de la sécurité nationale peuvent avoir accès et utiliser les données stockées sans l'autorisation de l'instance judiciaire. Ainsi, la Loi n° 51/1991 sur la sécurité nationale de la Roumanie, republiée au Moniteur officiel de la Roumanie, Partie I, n° 190 du 18 mars 2014, prévoit, à l'article 8, les organes de l'État avec attributions dans le domaine de la sécurité nationale, ceux-ci étant le Service Roumain de Renseignements, le Service de Renseignements Extérieurs et le Service de Protection et de Garde, et à l'article 9, il dispose que le Ministère de la Défense Nationale, le Ministère de l'Intérieur et Ministère de la Justice organisent des structures de renseignements avec attributions spécifiques à leurs domaines d'activité. La Cour constate, par ailleurs, qu'aux termes de l'article 13, point e) de la loi, les organes avec des attributions dans le domaine de la sécurité nationale peuvent, dans les conditions de l'existence de menaces à l'encontre de la sécurité nationale de la Roumanie, telles que définies par l'article 3 de la Loi n° 51/1991, demander l'obtention des données générées ou traitées par les fournisseurs de réseaux publics, de communications électroniques ou les fournisseurs de services de communications électroniques accessibles au public, autres que leur contenu, et conservées par eux en vertu de la loi, sans que cet article ou l'article 14 de la loi prévoit que cette demande doit être autorisée par un juge.

14. La Cour note également qu'en vertu de l'article 9 de la Loi n° 14/1992 sur l'organisation et le fonctionnement du Service Roumain de Renseignements, « afin d'établir l'existence de menaces à l'encontre de la sécurité nationale, prévue à l'article 3 de la Loi n° 51/1991 sur la sécurité nationale de la Roumanie, tel que modifiée, les services de renseignements peuvent effectuer, en conformité avec la loi, des vérifications par : [...] e) l'obtention des données générées ou traitées par les fournisseurs de réseaux publics de communications électroniques ou par les fournisseurs de services de communications électroniques accessibles au public, autres que leur contenu, et conservées par ceux-ci conformément à la loi. » Mais, tout comme les dispositions de la Loi n° 82/2012 et de la Loi n° 51/1991, ni les dispositions de la Loi n° 14/1992 ne prévoient l'obligation de ce service de renseignements d'obtenir l'autorisation du juge pour avoir accès aux données stockées.

15. La Cour estime aussi que la Loi n° 1/1998 sur l'organisation et le fonctionnement du Service de Renseignements Extérieurs, republiée au Moniteur officiel de la Roumanie, Partie I, n° 511 du 18 Octobre 2000, prévoit à l'article 10, paragraphe (1) que « *Le Service de Renseignements Extérieurs est autorisé à utiliser des personnes morales d'infiltration, créées dans les conditions de la loi, à utiliser des méthodes spécifiques, à créer et posséder des moyens appropriés pour obtenir, vérifier, protéger, évaluer, valoriser et stocker des données et des informations relatives à la sécurité nationale* » et, selon le paragraphe (3) du même article, « *l'utilisation des moyens d'obtention, de vérification et de valorisation des données et des informations ne doit aucunement porter atteinte aux droits fondamentaux ou aux libertés fondamentales des citoyens, à la vie privée, à leur honneur ou réputation ou les soumettre à des restrictions illégales* ». En outre, conformément à l'article 11 de la Loi n° 1/1998, « *Le Service de Renseignements Extérieurs a le droit, dans les conditions de la loi, de demander et d'obtenir, des autorités publiques roumaines, des agents économiques, d'autres personnes*

morales, et des personnes physiques, des informations, des données ou des documents nécessaires pour exercer ses fonctions ». Par conséquent, la Cour constate que la Loi n° 1/1998 ne régit pas de manière spécifique l'accès du Service de Renseignements Extérieurs aux données conservées par les fournisseurs de réseaux publics de communications électroniques et les fournisseurs de services de communications électroniques accessibles au public, cet accès étant régi par l'article 13 de la Loi n° 51/1991, sans être conditionné, donc, par l'autorisation préalable d'une instance judiciaire.

16. Or, l'absence de ce types d'autorisations a été aussi critiquée, parmi d'autres, par la Cour de Justice de l'Union européenne dans l'Arrêt du 8 avril 2014, ce manque équivalant à l'insuffisance des garanties procédurales nécessaires à la protection du droit à la vie privée et des autres droits consacrés par l'article 7 de la Charte des droits fondamentaux et des libertés fondamentales et du droit fondamental à la protection des données à caractère personnel, consacré par l'article 8 de la Charte (alinéa 62).

17. Pour toutes ces raisons, la Cour a fait droit à l'exception d'inconstitutionnalité soulevée par le Tribunal de Première Instance Constanța – Section pénale, d'office, et a constaté que les dispositions de la Loi n° 82/2012 sur la conservation des données générées ou traitées par les fournisseurs de réseaux publics de communications électroniques et les fournisseurs de services de communications électroniques accessibles au public, et portant modification et complément de la Loi n° 506/2004 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques étaient inconstitutionnelles. En outre, la Cour a constaté que les dispositions de l'article 152 du Code de procédure pénale étaient constitutionnelles par rapport aux critiques formulées.