26 septembre 2024

Cour constitutionnelle

COMMUNIQUÉ DE PRESSE
ARRÊT 97/2024

La Cour rejette en partie les recours contre la nouvelle loi sur les communications électroniques et pose plusieurs questions préjudicielles à la Cour de justice de l'Union européenne avant de répondre aux griefs restants

Plusieurs organismes et associations ainsi que des particuliers demandent l'annulation de la nouvelle loi du 20 juillet 2022 relative à la conservation des données en matière de communications électroniques. Cette loi s'inscrit dans le prolongement de la loi du 29 mai 2016, qui avait un objet similaire et qui avait été annulée par la Cour. Les critiques des parties requérantes concernent différents aspects de la nouvelle loi et la compatibilité de celle-ci avec le droit au respect de la vie privée et à la protection des données à caractère personnel.
La Cour rejette une partie importante de ces critiques, compte tenu du cadre établi par le législateur et des garanties qu'il a prévues. Concernant les communications couvertes par le secret professionnel, la Cour indique que la loi doit être interprétée d'une certaine manière. En ce qui concerne la conservation des données de trafic et des données de localisation, la Cour pose plusieurs questions préjudicielles à la Cour de justice de l'Union européenne (CJUE). La Cour statuera sur les griefs restants une fois que la CJUE aura répondu aux questions.

1. Contexte de l'affaire

La loi du 20 juillet 2022 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques et à la fourniture de ces données aux autorités » vise principalement à répondre l'annulation par la Cour de la loi du 29 mai 2016, qui avait un objet similaire (arrêt n° 57/2021). À la suite de cet arrêt, le législateur a dû élaborer une nouvelle réglementation sur la conservation des données relatives aux communications électroniques en respectant les principes applicables, à la lumière de la jurisprudence de la CJUE.

L'Ordre des barreaux francophones et germanophone, l'ASBL « Académie Fiscale », l'ASBL « Liga voor Mensenrechten », l'ASBL « Ligue des Droits humains », une fondation ayant pour objet la protection de la vie privée et des particuliers demandent l'annulation de la nouvelle loi.

2. Examen par la Cour

Les parties requérantes soulèvent plusieurs griefs concernant différents aspects de la loi attaquée. Ces griefs concernent principalement la compatibilité de cette loi avec le droit au respect de la vie privée et à la protection des données à caractère personnel.

2.1. L'utilisation de la cryptographie (article 3)

La loi attaquée établit plusieurs exceptions à la libre utilisation de la cryptographie en matière de communications électroniques. Ces exceptions visent à éviter qu'un opérateur ne puisse pas exécuter une demande ciblée d'une autorité dans le but d'identifier l'utilisateur final ou de repérer des communications non accessibles au public et à éviter qu'un opérateur étranger empêche l'exécution d'une demande d'une autorité lorsque l'utilisateur final ou l'abonné est en Belgique. Les parties requérantes contestent ces deux exceptions. **La Cour rejette la critique**, dès lors que l'objectif du législateur est légitime, que les données concernées sont déterminées avec précision et qu'elles ne portent pas sur le contenu de la communication.

2.2. Les mesures employées au niveau du réseau ou de l'utilisateur final pour détecter la fraude et les utilisations malveillantes des réseaux et des services (article 4)

Certaines parties requérantes critiquent la possibilité pour les opérateurs de mettre en œuvre des mesures de blocage et de désactivation en vue de détecter les fraudes et utilisations malveillantes et d'éviter que les utilisateurs en subissent un préjudice. Selon elles, cette faculté viole la liberté d'expression et d'information. **La Cour rejette cette critique**, dès lors que la mesure attaquée poursuit des objectifs légitimes et qu'elle est proportionnée à ces objectifs. Les opérateurs agissent dans ce cadre sous le contrôle de l'Institut belge des services postaux et des télécommunications (IBPT), qui peut leur donner des instructions contraignantes.

2.3. La conservation des données de trafic (article 5)

Les parties requérantes critiquent l'obligation pour les opérateurs de conserver des données de trafic en vue d'agir contre les fraudes et utilisations malveillantes du réseau ou d'assurer la sécurité ou le bon fonctionnement du réseau ou des services de communications électroniques.

La Cour juge que la mesure attaquée poursuit des objectifs légitimes. Cependant, avant de statuer sur le caractère proportionné de la mesure, **la Cour pose une question préjudicielle à la CJUE** sur la possibilité pour les Etats membres de prendre des mesures de conservation de données en vue d'assurer la prévention, la recherche, la détection et la poursuite d'utilisations non autorisées du système de communications électroniques.

2.4. La conservation des données de localisation (article 6)

Certaines parties requérantes critiquent la possibilité pour les opérateurs de réseaux mobiles de conserver des données de localisation autres que les données de trafic. Avant de statuer sur cette critique, **la Cour décide d'interroger la CJUE** sur les finalités de cette obligation, ainsi que sur la possibilité de maintenir provisoirement les effets de la mesure en cas d'annulation.

2.5. La conservation des données de souscription et d'identification (article 8)

Plusieurs parties requérantes critiquent l'obligation pour les opérateurs de conserver certaines données de souscription et d'identification. La Cour relève que la CJUE a admis qu'une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs pouvait être imposée à des fins plus larges (sauvegarde de la sécurité nationale et de la sécurité publique, ainsi que dans le cadre de la lutte contre la criminalité, grave ou non) que les finalités requises pour la conservation des adresses IP attribuées à une source de connexion. En l'occurrence, le législateur a énuméré les données qui doivent être conservées, les finalités et le délai de conservation. Ces finalités correspondent aux finalités identifiées par la CJUE. Par ailleurs, la loi attaquée fixe des conditions strictes qui empêchent les opérateurs

et les autorités compétentes d'utiliser les adresses IP pour effectuer le traçage exhaustif d'un internaute. **La Cour rejette donc les critiques** des parties requérantes.

2.6. L'obligation d'identification des abonnés et des utilisateurs finaux (article 12)

Diverses parties requérantes critiquent l'obligation pour les opérateurs d'identifier les abonnés, ce qui implique la conservation de certaines données. La Cour relève que les données concernées visent à identifier les abonnés et à lutter contre la fraude à l'identité. En ce qui concerne l'obligation de conserver certaines adresses IP, la Cour rejette la critique pour les mêmes raisons que celles mentionnées au point 2.5. Les autres données peuvent quant à elles être assimilées à des données relatives à l'identité civile des utilisateurs, dès lors qu'elles ne permettent pas de connaître des détails d'une communication ni donc d'établir un profil de l'utilisateur et de suivre ses mouvements. Compte tenu des différentes garanties prévues par la disposition attaquée, **la Cour rejette les critiques** soulevées à ce sujet. Selon la Cour, les recours juridictionnels ordinaires permettent d'assurer un contrôle suffisant.

Certaines parties requérantes soutiennent également que la règle selon laquelle, sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques viole le droit à un procès équitable et la présomption d'innocence. **La Cour rejette également cette critique**. Selon elle, la règle attaquée ne fait que rappeler la présomption de départ de toute enquête, et il y a lieu de l'écarter dès qu'elle est contredite par des preuves. Par ailleurs, un prévenu peut contester cette présomption par toutes voies de droit.

Est aussi critiquée la possibilité pour l'opérateur ou le point de vente d'utiliser une technologie de reconnaissance faciale pour identifier les abonnés. Selon la Cour, la possibilité de réaliser, d'une manière automatique, une comparaison entre les données biométriques de la photo du document d'identification et le visage de l'abonné est pertinente en vue d'identifier l'abonné, quand bien même la fiabilité totale du procédé ne serait pas garantie. L'exécution de la mesure s'accompagne de diverses garanties au profit de l'abonné, et notamment la possibilité pour celui-ci de recourir à une autre manière de s'identifier. **La Cour rejette donc le grief**.

2.7. La conservation ciblée de données sur la base d'un critère géographique (articles 9 à 11)

La loi du 20 juillet 2022 oblige les opérateurs à conserver certaines données de trafic et de localisation à des fins de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave, de prévention de menaces graves contre la sécurité publique et de sauvegarde des intérêts vitaux d'une personne physique dans cinq types de zones géographiques. Ces zones sont définies notamment sur la base du taux d'infractions graves qui y commises, du niveau de menace, ou encore d'un risque de menace grave spécifique concernant une série de lieux limitativement énumérés. Plusieurs parties requérantes critiquent cette mesure.

La Cour relève que la CJUE a admis la faculté de délimiter la conservation de données sur la base d'un critère géographique. Certes, le nombre et la variété des zones visées sont considérables, de sorte qu'il n'est pas exclu que tout ou une partie importante du territoire soit couverte. Cela ne signifie toutefois pas que la mesure s'assimile à une mesure généralisée et indifférenciée de conservation des données. Les critères retenus par le législateur pour définir ces zones sont pertinents et le législateur s'est limité au strict nécessaire. **La Cour rejette donc la critique**.

2.8. L'énumération des autorités compétentes et des finalités dans le cadre de l'accès aux données (article 13)

Plusieurs parties requérantes critiquent l'énumération des autorités susceptibles d'accéder aux données, qui serait laissée à l'appréciation du ministre compétent et qui serait trop large, ainsi que les finalités d'un tel accès. **La Cour relève qu'une partie des griefs ne découle pas de la disposition attaquée mais de normes législatives distinctes**. La Cour précise que la disposition attaquée vise uniquement à permettre au ministre de reprendre dans une circulaire l'ensemble des autorités visées par ces autres normes législatives.

2.9. Les compétences de diverses autorités (articles 24 à 27)

Une partie requérante critique les compétences conférées aux officiers de police judiciaire de l'IBPT, au procureur du Roi et au juge d'instruction.

En ce qui concerne ***les agents de l'IBPT***, **la Cour sursoit à statuer dans l'attente de la réponse de la CJUE** aux questions préjudicielles mentionnées plus haut.

En ce qui concerne la faculté pour ***le procureur du Roi*** d'ordonner à un opérateur de conserver des données qu'il juge nécessaire pour certaines infractions (article 39*quinquies* du Code d'instruction criminelle), **la Cour juge que la partie requérante ne démontre pas en quoi le législateur aurait excédé sa marge d'appréciation** en définissant la notion de criminalité grave par référence aux infractions susceptibles de donner lieu à un emprisonnement d'un an ou à une peine plus lourde. Du reste, le rattachement d'une infraction pénale à la criminalité grave doit s'apprécier de façon concrète, sous le contrôle du juge pénal. En outre, le procureur du Roi doit démontrer que le délai de conservation qu'il impose est limité au strict nécessaire, sous le contrôle du juge pénal. **La critique** faite à la possibilité pour le procureur du Roi de procéder à l'identification de l'abonné (article 46*bis* du Code précité) **est rejetée** pour les mêmes motifs que ceux mentionnés au point 2.5. Enfin, ni la CJUE ni la Cour européenne des droits de l'homme n'exigent la mise en place d'un contrôle judiciaire ou administratif préalable de l'accès aux données ou d'un recours spécifique, ni l'information de l'intéressé.

Enfin, en ce qui concerne la possibilité pour ***le juge d'instruction*** de requérir des données de trafic et de localisation pour certaines infractions (article 88*bis*, § 2, du Code d'instruction criminelle), la partie requérante considère que l'accès aux données ne se limite pas à la criminalité grave. **La Cour rejette cette critique** pour les mêmes motifs que ceux concernant l'accès du procureur du Roi à certaines données. La Cour relève que le juge d'instruction est un magistrat indépendant et impartial dont l'intervention est une garantie essentielle pour le respect de la vie privée. Les recours ordinaires à l'encontre d'une ordonnance du juge d'instruction suffisent en la matière. Quant à l'information de la personne concernée, elle se fait conformément aux règles du Code d'instruction criminelle applicable à l'instruction.

2.10. Les compétences des services de renseignement et de sécurité (articles 33, 34 et 37)

Une autre partie requérante critique les compétences que la loi attaquée confère aux services de renseignement et de sécurité. En ce qui concerne la compatibilité des dispositions attaquées avec le droit au respect de la vie privée (article 22 de la Constitution), la Cour relève que le législateur a précisé les catégories de données qui peuvent être traitées par les services de renseignement et de sécurité, et que l'ingérence est suffisamment prévisible. **La Cour rejette donc la critique**.

2.11. La protection du secret professionnel

Plusieurs parties requérantes critiquent l'absence de protection des informations couvertes par le secret professionnel. La Cour relève qu'en dehors de l'article 88*bis*, § 3, du Code d'instruction

criminelle, qui vise les prérogatives du procureur du Roi concernant les communications entre l'avocat, le médecin et leurs clients ou patients, la loi du 20 juillet 2022 ne prévoit pas de protection particulière pour les données couvertes par le secret professionnel. Selon la Cour, cet article 88*bis*, § 3, doit cependant **s'interpréter comme obligeant le procureur du Roi à avertir le bâtonnier ou le représentant de l'ordre des médecins avant l'exécution de la mesure pour que celui-ci puisse examiner préalablement les éléments que le procureur du Roi veut consulter et lui faire les recommandations nécessaires**. La Cour ajoute que cette réserve d'interprétation vaut de manière similaire pour toutes les données couvertes par le secret professionnel, et donc pour d'autres catégories de professionnels, selon les modalités et dans les conditions prévues par le législateur. Le secret professionnel ne peut céder, dans chaque cas concret où une autorité a accès aux données conservées, que si un motif d'intérêt général le justifie et que la levée du secret est strictement proportionnée à cet objectif. Dès lors, la loi attaquée ne porte pas une atteinte discriminatoire au secret professionnel.

3. Conclusion

La Cour pose plusieurs questions préjudicielles à la CJUE. Sous réserve de l'interprétation mentionnée au point 2.11, elle rejette les autres critiques.

La Cour constitutionnelle est la juridiction qui veille au respect de la Constitution par les différents législateurs en Belgique. La Cour peut annuler, déclarer inconstitutionnels ou suspendre des lois, des décrets ou des ordonnances en raison de la violation d'un droit fondamental ou d'une règle répartitrice de compétence.

Ce communiqué de presse, rédigé par la cellule « médias » de la Cour, ne lie pas la Cour constitutionnelle. Le texte de l'arrêt est disponible sur le site web de la Cour constitutionnelle.

Contact presse : Martin Vrancken | 02/500.12.87 | Romain Vanderbeck | 02/500.13.28

Suivez la Cour via X @ConstCourtBE et LinkedIn