Avis de la Ligue des Droits Humains sur le projet de loi du 17 mars 2022 relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités – DOC 552572/001

Avril 2022

A l'attention de la commission de l'Économie, de la Protection des Consommateurs et de l'Agenda numérique de la Chambre des représentants.

Votre courrier du 31 mars dernier adressé à la Ligue des Droits Humains (ci-après LDH) a retenu toute notre attention. Nous saluons une fois encore la volonté de la commission de s'entourer d'avis extérieurs dans le cadre de ses travaux et vous remercions pour la confiance dont votre consultation témoigne à notre égard.

I. Introduction

La conservation généralisée des métadonnées[1] est une mesure qui consiste pour les opérateurs et fournisseurs de réseaux et services de communications électroniques en la collecte et le stockage systématiques et a priori de données traitées et générées lors d'une communication électronique à l'exception de leur contenu. En ce qu'elle implique une ingérence particulièrement grave dans le droit au respect de la vie privée et à la protection des données à caractère personnel, cette technique est controversée[2].

La LDH s'est levée à de nombreuses reprises contre les tentatives d'introduire une telle obligation[3].

---

[1] Définies comme « les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication. ».

[2] Pour une analyse voy. C. FORGET, « L'obligation de conservation des « métadonnées » : la fin d'une longue saga juridique ? », *J.T.,* 2017/13, n° 6683, pp. 233-239 ; M. PANZAVOLTA, S. ROYER et H. SEVERIJNS, « Algemene dataretentie: ten minste houdbaar tot ...? », *T.Strafr.* 2018, afl. 1, pp. 2-16.

[3] Voy. notamment :
- Vie privée : la Cour constitutionnelle donne à nouveau raison à la LDH et ses partenaires en annulant partiellement la loi sur la conservation des métadonnées de communication (2021) https://www.liguedh.be/vie-privee-la-cour-constitutionnelle-donne-a-nouveau-raison-a-la-ldh-et-ses-partenaires-en-annulant-partiellement-la-loi-sur-la-conservation-des-metadonnees-de-communication/

En 2015, suite à un recours en annulation introduit conjointement par la Ligue des droits humains, la Liga voor mensenrechten et l'Ordre des barreaux francophones et germanophone[4], la Cour constitutionnelle[5] annulait la 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 90*decies* du Code d'instruction criminelle[6] transposant la directive européenne 2006/24/CE[7], elle-même précédemment invalidée par la Cour de justice de l'Union européenne (ci-après « CJUE ») dans son arrêt *Digital Rights*[8]. Cette annulation devait mettre fin à l'obligation qui imposait aux opérateurs de télécommunications et aux fournisseurs d'accès à internet de conserver, à des fins de lutte contre la criminalité grave, toutes les informations de trafic concernant les usagers de ces télécommunications (aussi appelées « métadonnées »), soit une collecte massive et indiscriminée de données à caractère personnel.

Malgré cette première annulation, l'Etat belge a adopté une nouvelle législation similaire[9] qui, si elle ne présentait pas toutes les tares de la première, n'en imposait pas moins une collecte systématique et massive des métadonnées des personnes présentes sur le territoire belge[10]. A nouveau, la LDH, la Liga voor mensenrechten et Avocats.be, aux côtés d'autres parties, ont réitéré leur demande à la Cour constitutionnelle d'annuler cette norme législative. Celle-ci se tourna vers la CJUE. En octobre 2020, la CJUE suivait les arguments de la Ligue des droits humains et confirmait que le droit communautaire s'oppose à une législation nationale qui oblige les opérateurs de télécommunication à conserver les données de tous les utilisateurs, sans distinction, pendant des périodes pouvant aller jusqu'à 12 mois. En conséquence, l'arrêt de la Cour constitutionnelle d' avril 2021[11] annula partiellement la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques. Il s'agissait de la 4ème décision d'une instance suprême sur cette thématique.

***

- Arrêt de la Cour de justice de l'UE du 6 octobre 2020 sur la loi relative à la conservation des données : une nouvelle victoire pour la protection des données (2020) https://www.liguedh.be/arret-de-la-cour-de-justice-de-lue-du-6-octobre-2020-sur-la-loi-relative-a-la-conservation-des-donnees-une-nouvelle-victoire-pour-la-protection-des-donnees/
- Avis sur le projet de loi Data Retention 2.0 (2016) : https://www.liguedh.be/avis-sur-le-projet-de-loi-data-retention-20/
- La directive sur la conservation des données, son invalidation et les obligations de la Belgique (2015) : https://www.liguedh.be/la-directive-sur-la-conservation-des-donnees-son-invalidation-et-les-obligations-de-la-belgique-2/
- Directive Data Retention : position et enjeux (2011) https://www.liguedh.be/transposition-de-la-directive-europeenne-sur-la-conservation-des-donnees-un-danger-pour-la-vie-privee-et-la-democratie-2/

[4] Ancienne dénomination d'Avocats.be.
[5] C.C., 11 juin 2015, n° 84/2015.
[6] *M.B.,* 23 août 2013.
[7] 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, Journal officiel de l'Union européenne (ISSN 1725-2563), 13 avril 2006, p. 54.
[8] C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 & C-594/12.
[9] Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016.
[10] Pour une analyse, voir Avis de Datapanik, la Liga voor Mensenrechten, la Ligue des droits de l'Homme et la NURPA concernant le projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques (DOC 54 1567/001), 15 février 2016, https://nurpa.be/files/20160215_avis-associations-droits-homme-projet-loi-conservation-donnees.pdf.
[11] C.C., 22 avril 2021, n°57/2021.

II. Evolution de la jurisprudence européenne

Par divers arrêts[12], la CJUE a rappelé que la conservation des métadonnées constituait, en elle-même, une dérogation au principe de confidentialité des communications inscrit dans l'article 5, §1 de la directive 2002/58/CE. Cette mesure doit rester l'exception, et non la règle[13]. Constituant une ingérence « d'une vaste ampleur et d'une gravité particulière », elle préconise qu'elle soit « précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire » [14].

Elle a également établi que le législateur peut déroger à l'interdiction de la surveillance généralisée, mais uniquement **en cas de menace grave pour la sécurité nationale** et à condition que la conservation des données soit limitée dans le temps, dans la mesure strictement nécessaire, que des garanties suffisantes soient prévues et que le contrôle de l'accès soit entre les mains d'un tribunal ou d'une autorité administrative indépendante. Ces législations doivent contenir des garanties suffisantes permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En d'autres mots, "la Charte, ne s'oppose pas à des mesures législatives permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace". Mais attention, la Cour limite la possibilité d'une conservation généralisée et indifférenciée des métadonnées, aux conditions susmentionnées, pour la finalité de sauvegarde de la sécurité nationale.

En ce qui concerne la lutte contre la criminalité grave, la Cour impose un changement de perspective : l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. Et à raison: pour ce qui est de la collecte de preuves électroniques de toute infraction pénale, le standard international en la matière, à savoir la Convention de Budapest, ne requiert que la conservation rapide des données de trafic *a posteriori*, c'est-à-dire après une injonction judiciaire. C'est donc de manière dérogatoire à ce standard international et en exception au droit à la confidentialité inscrit dans l'article 5, §1 de la directive 2002/58/CE, qu'il s'agit de lire le raisonnement de la CJUE en matière de lutte contre la criminalité grave. Pour ce versant, la CJUE s'est référée aux alternatives disponibles à une conservation générale de toutes les données, telles que 1) la conservation des données relatives au trafic et des données de localisation fondée sur un critère géographique sur la base d'éléments objectifs et non discriminatoires, 2) la conservation généralisée

[12] l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) (Privacy International, C-623/17), le Conseil d'État (France) (La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18) ainsi que la Cour constitutionnelle (Belgique) (Ordre des barreaux francophones et germanophone e.a., C-520/18)

[13] CJUE, n° C-511/18, Arrêt (JO) du 6 octobre 2020, dit arrêt *Quadrature du Net*. Point 142

[14] Point 65 de l'arrêt *Digital Rights*.

et indifférenciée des seules adresses IP attribuées et 3) un “gel rapide” des données détenues par les fournisseurs de télécommunications.

Concernant le point 1) la Cour admet la conservation ciblée et a priori des données de trafic et de localisation à fins de lutte contre la criminalité grave sur la **base d’éléments objectifs et non discriminatoires et ce, pour une durée limitée au strict nécessaire**[15], estimant également qu’il revient au législateur de fixer dans la réglementation « des **éléments objectifs** permettant de **viser un public** dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d’une manière ou d’une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique »[16]. En d’autres mots, la Charte, ne s’oppose pas à des mesures législatives prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d’éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d’un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelables. La Cour constitutionnelle fera siens ces arguments en relevant à l’instar de la CJUE que « l’obligation de conservation des données relatives aux communications électroniques doit être l’exception, et non la règle » et ordonnera l’annulation partielle de la loi du 29 mai 2016 qui repose « dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l’ensemble des données visées » [17].

Concernant le point 2) tout en ayant admis par exception la conservation ciblée et a priori des données de trafic et de localisation, la Cour innove en autorisant la conservation systématique et indifférenciée des adresses IP attribuées à la source d’une communication électronique. La Cour considère en effet que la collecte de ces données présente « un degré de sensibilité moindre que les autres données de trafic » et qu’il peut s’agir du seul moyen d’identifier « la personne à laquelle cette
adresse était attribuée au moment de la commission de cette infraction ». Néanmoins, eu égard à la gravité de l’ingérence — « les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d’un internaute et, par suite, de son activité en ligne, ces données permettent d’établir le profil détaillé de ce dernier »—, seule la lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique sont de nature à justifier cette ingérence. En sus, la Charte ne s’oppose pas à des mesures législatives prévoyant une conservation généralisée et indifférenciée des adresses IP attribuées à la source d’une connexion que si une période temporellement limitée au strict nécessaire est prévue.

Concernant le point 3), la Cour admet que la Charte, ne s’oppose pas à des mesures législatives permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d’une décision de l’autorité compétente soumise à un contrôle juridictionnel

[15] Points 147-148 de l’arrêt *Quadrature du Net*.
[16] Point 148 de l’arrêt *Quadrature du Net* et point 111 de l’arrêt *Tele2.*
[17] C.C., 22 avril 2021, n° 57/2021, point B.17-18. Voir également LDH, « Vie privée : la Cour constitutionnelle donne à nouveau raison à la LDH et ses partenaires en annulant partiellement la loi sur la conservation des métadonnées de communication », 23 avril 2021, https://www.liguedh.be/vie-privee-la-cour-constitutionnelle-donne-a-nouveau-raison-a-la-ldh-et-ses-partenaires-en-annulant-partiellement-la-loi-sur-la-conservation-des-metadonnees-de-communication/.

effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

Toutes les mesures visées du point 1) au point 3) doivent assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

Le 5 avril dernier, dans son arrêt Garda Síochána de la CJUE du 5 avril 2022[18], la CJUE a réitéré sa position dans le volet de lutte contre la criminalité grave tout en en précisant les contours. Elle rappelle que le droit de l'Union « s'oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.»[19] Elle précise qu' « *aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique* »[20], « *dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus* »[21], le droit de l'Union ne s'oppose pas à des mesures législatives prévoyant :

- une conservation ciblée des **données relatives au trafic et des données de localisation** qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires,
  - en fonction de catégories de personnes concernées
  - ou au moyen d'un critère géographique,
  - pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

- une conservation généralisée et indifférenciée **des adresses IP attribuées à la source d'une connexion**,
  - pour une période temporellement limitée au strict nécessaire ;

- une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ;

- le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation rapide **des données relatives au trafic et des données de localisation** dont disposent ces fournisseurs de services,
  - pour une durée déterminée,
  - au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif.

***

[18] ARRÊT DE LA COUR (grande chambre), 5 avril 2022, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62020CJ0140&qid=1652092196283
[19] Idem, Point 101
[20] Idem, point 1 *du dispositif de l'arrêt.*
[21] Idem, point 1 *in fine, du dispositif de l'arrêt.*

III. Examen du projet de loi

1. Une distinction importante à clarifier

L'avant-projet de loi en question a fait l'objet d'un avis fouillé très sévère de la part de l'Autorité de protection des données (APD)[22]. Celle-ci relève des risques importants pour le respect des droits fondamentaux, que ce soit d'un point de vue de la légalité, de la nécessité ou de la proportionnalité[23].

Dans ces différents arrêts et en conformément à l'article 52, §1 de la Charte, la CJUE ne s'oppose pas à des mesures législatives poursuivant des objectifs sécuritaires pour autant que celles-ci soient « rigoureusement » proportionnées au but poursuivi et opèrent dans les limites du strict nécessaire. La CJUE laisse aux législateurs le soin « d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire. » et qu'il existe « un rapport entre les données à conserver et l'objectif poursuivi ». Elle ne dit pas autre chose dans son récent arrêt Garda Síochána en précisant que « le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation rapide des données relatives au trafic et des données de localisation » ne peut l'être que pour une "durée déterminée", et "résulter d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif".

Ainsi que nous l'avons déjà rappelé dans notre examen de la jurisprudence européenne, la CJUE opère une distinction fondamentale entre les finalités pouvant être poursuivies et, par conséquent, selon la finalité poursuivie, l'étendue de la collecte de métadonnées pouvant être effectuée. En somme, la Cour permet, à certaines conditions rappelées plus haut, la collecte généralisée et indifférenciée des métadonnées à des fins de sauvegarde de la sécurité nationale, mais consacre le principe de la fin de l'obligation de conservation systématique et indifférenciée de ces données à des fins de lutte contre la criminalité grave.

Cette analyse est confortée par un avis émis par le Professeur Vilenas Vadapala, ancien juge à la Cour de Justice de l'Union européenne, dans lequel celui-ci expose que la CJUE a autorisé les États membres à imposer la conservation générale et aveugle de tous les enregistrements détaillés des appels et des données de localisation uniquement lorsque cela était exceptionnellement nécessaire pour contrer une menace prévisible pour la sécurité nationale, telle qu'une attaque terroriste[24]. Il explique en quoi la France, dans ses tentatives d'instaurer un système de récolte de données comparable, a échoué à démontrer une menace spécifique pour la sécurité nationale autre qu'un risque général de terrorisme basé sur les attaques passées.

Dans son arrêt Guarda Síochána, la Cour confirme que la criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale.[25]

---

[22] Autorité de protection des données, Avis n° 108/2021 du 28 juin 2021 : https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf.

[23] *Ibid.*, pp. 71-75.

[24] https://www.patrick-breyer.de/wp-content/uploads/2022/04/20220407_Legal_Opinion_Data_Retention_Vadapalas_updated-SimeonTC-VV-REV.pdf

[25] Voir point 62 et 63: "Il convient, en outre, de relever que, à la différence de la criminalité, même particulièrement grave, une menace pour la sécurité nationale doit être réelle et actuelle ou, à tout le moins, prévisible, ce qui suppose la survenance de circonstances suffisamment concrètes, pour pouvoir justifier une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, pendant une durée limitée. Une telle menace se distingue donc, par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent, du risque général et permanent qu'est celui de survenance de tensions ou de troubles, même graves, à la sécurité publique ou celui d'infractions pénales graves (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-

Nous sommes d'avis que le projet de loi à l'examen mérite des clarifications plus précises quant à l'étendue de la collecte de métadonnées permise selon la finalité poursuivie.

2. LA LUTTE CONTRE LA CRIMINALITÉ GRAVE

a. Un choix politique

En matière de lutte contre la criminalité grave, le projet de loi à l'examen consiste, selon nous, avant tout en un choix politique désastreux. Des études démontrent que les lois sur la conservation des données n'ont eu d'effet mesurable sur le taux de criminalité ou le taux d'élucidation des crimes dans aucun pays de l'UE.

Par exemple, en 2011, une analyse du Arbeitkreis arbeit vorratsdatenspeicherung[26] a démontré qu'après deux années d'entrée en vigueur de la loi, la conservation des données n'avait pas rendu plus efficace la poursuite des crimes graves. En effet, si la conservation des données a permis à la police d'enregistrer plus d'actes criminels graves (2009 : 1 422 968) qu'avant (2007 : 1 359 102), les infractions graves ont cependant moins souvent été élucidées (2009 : 76,3%) qu'avant la conservation de toutes les données de communication (2007 : 77,6%).

Le comportement d'évitement des utilisateurs peut expliquer les effets contre-productifs de la conservation générale des données sur les enquêtes criminelles : afin d'éviter l'enregistrement d'informations sensibles dans le cadre d'un système de conservation générale des données, les utilisateurs ayant l'intention de protéger leurs communications ont recours à d'autres moyens tels qu'utiliser les cafés Internet, les points d'accès Internet sans fil, les services d'anonymisation, les téléphones publics, les cartes de téléphonie mobile non enregistrées, les canaux de communication non électroniques, etc.

L'exemple allemand a démontré que les enquêtes ciblées a posteriori peuvent, dans l'ensemble, être plus efficaces que la collecte d'informations sur les contacts, les mouvements et l'utilisation d'Internet de l'ensemble de la population. La conservation générale des données peut donc être contre-productive pour les enquêtes criminelles, en facilitant certaines d'entre elles, mais en rendant beaucoup plus futiles.

Récemment, le ministre de la Justice allemand aurait exprimé que le nouveau gouvernement souhaite modifier la réglementation allemande en matière de conservation des données afin qu'elle soit conforme aux droits constitutionnels européens et allemands en matière de protection de la vie privée[27].

520/18, EU:C:2020:791, points 136 et 137).
Ainsi, la criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale. En effet, comme M. l'avocat général l'a relevé aux points 49 et 50 de ses conclusions, une telle assimilation serait susceptible d'introduire une catégorie intermédiaire entre la sécurité nationale et la sécurité publique, aux fins d'appliquer à la seconde les exigences inhérentes à la première.

[26] "Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics", 2011, https://www.statewatch.org/media/documents/news/2011/jan/dret-working-party-report-on-germany.pdf

[27] *Allemagne : La rétention des données doit être abolie une fois pour toutes.* 29/12/2021 https://tutanota.com/fr/blog/posts/data-retention-germany/

b. L'obligation de collecter certaines données de trafic et/ou de localisation

Le projet à l'examen entend imposer aux opérateurs qui offrent des services de communications électroniques, ainsi qu'aux opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, la collecte de certaines données, dont:

- les données de souscription des abonnés[28] ainsi que leurs données d'identification[29],
- Les métadonnées de communications électroniques, en ce compris l'origine et la destination de la communication et la localisation de l'équipement terminal

1. Collecte des données de souscription de l'abonné et données d'identification

L'article 126, §1er de la loi tel que modifié par le projet de loi à l'examen prévoit d'imposer la collecte systématique et indifférenciée de « données de souscription de l'abonné au service ainsi que des données qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé. » Il délègue au Roi le soin de déterminer les données à conserver ainsi que les exigences auxquelles ces données doivent répondre tout en prévoyant que cette collecte ne peut porter sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication ou sur la localisation de l'équipement terminal.

Cependant, l'arrêté royal du 19 septembre 2013 tel que modifié par le projet d'arrêté soumis pour avis à l'Autorité de protection des données permet la récolte de données non visées par la CJUE et dépassant la marge laissée par la Cour, tels que l'IMEI (International Mobile Equipment Identity), l'IMSI (International Mobile Subscriber Identity), l'ICCID (Integrated Circuit Card Identifier), l'adresse MAC, le MSISDN (Mobile Station Integrated Services Digital Network), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées". Or cela ne semble pas conforme à la jurisprudence établie dans par la CJUE dans ses arrêts des 6 octobre 2020 et 5 avril 2022 par lesquels elle insiste pour que ne soit octroyée comme exception que la conservation systématique et indifférenciée des « adresses IP » à la source d'une communication électronique.

Dans son arrêt du 6 octobre 2020[30], la CJUE a estimé que la conservation généralisée des adresses IP attribuées à la source d'une connexion constitue une ingérence grave dans les droits fondamentaux des internautes mais qu'une telle conservation préventive généralisée pouvait s'avérer nécessaire parce que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. Toutefois, eu égard à la gravité de l'ingérence, la Cour estime que seul un objectif suffisamment important, à l'instar de la lutte contre la criminalité grave, peut justifier une telle mesure de conservation généralisée des adresses IP.

---

[28] Produits auxquels l'abonné a souscrit, le début et la fin du service ainsi que les identifiants et différents numéros qui lui sont attribués lors de la souscription au service.

[29] nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé.

[30] Arrêt de la Cour (grande chambre) du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a. Affaires jointes C-511/18, C-512/18 et C-520/18

En effet, l'adresse IP est, dans la plupart des cas, suffisante pour permettre l'identification pseudonymique. C'est d'ailleurs en ce sens qu'elle précise, dans l'arrêt Garda Síochána[31], que « la conservation généralisée des adresses IP de la source de la connexion constitue une ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte dès lors que ces adresses IP peuvent permettre de tirer des conclusions précises sur la vie privée de l'utilisateur du moyen de communication électronique concerné et peut avoir des effets dissuasifs sur l'exercice de la liberté d'expression garantie à l'article 11 de celle-ci. » Mettant néanmoins en balance les droits et des intérêts légitimes en cause, et prenant pour exemple le cas d'une infraction commise en ligne et, en particulier, dans le cas de l'acquisition, de la diffusion, de la transmission ou de la mise à disposition en ligne de pédopornographie, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction.

Il faut dès lors considérer qu'en imposant aux fournisseurs d'un service de téléphonie mobile accessible au public, la conservation de, notamment, l'identifiant créé pour chaque communication, la date de début de l'abonnement ou de l'enregistrement au service, les données relatives au type de paiement ou encore, le numéro d'identification du terminal de l'utilisateur final (« International Mobile Equipment Identity », « IMEI », l'adresse « MAC (Media Access Control) » ou « Permanent Equipment Identifier (PEI) »), le législateur dépasse le champ d'application de l'exception définie par la CJUE qui se limite aux adresses IP.

De plus, le législateur manque également à l'obligation d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation et de justifier qu'il existe « un rapport entre les données à conserver et l'objectif poursuivi » de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire ».

Enfin, en ce qui concerne la conservation des adresses IP en tant que telles, la CJUE admet la « conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ». Cet élément temporel n'est pas précisé dans le projet de loi à l'examen, ce qui conduit à rendre la disposition disproportionnée. De plus, les nouvelles caractéristiques de l'IPv6 n'avaient pas encore été prises en compte par la CJUE quand elle permettait cette conservation des adresses IP, ce qui devrait conduire le législateur à la prudence et la nuance quand il la prévoit. En effet, dans le contexte de l'Internet des Objets, les adresses IP sont liées à énormément d'accessoires de tous les jours, ce qui rend cette collecte - en tant que telle - d'autant plus intrusive.

2. *Les métadonnées de communications électroniques, en ce compris l'origine et la destination de la communication et la localisation de l'équipement terminal*

2.1 La lutte contre la fraude et l'utilisation malveillante n'est pas de la criminalité grave

L'article 122, §4, 1° à 4° de la loi tel que modifié par le projet de loi à l'examen impose notamment aux opérateurs une conservation préventive systématique des données reprises dans le « Call detail record » (CDR) ou un registre fonctionnellement équivalent, ainsi que les données de localisation de l'auteur d'une fraude présumée ou d'une utilisation malveillante mais aussi des données de trafic nécessaires aux fins de détecter une fraude présumée ou une utilisation malveillante présumée du réseau de communications électroniques.

[31] ARRÊT DE LA COUR (grande chambre), 5 avril 2022, Point 73

Le système prévu par la loi, étant particulièrement intrusif, ne remplit pas ces critères et paraît manifestement disproportionné. La CJUE a rappelé, dans son arrêt Garda Síochána, que « s*'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général ».*

2.2. collecte ciblée moyennant un critère géographique

Comme rappelé par la jurisprudence européenne, la collecte des métadonnées de communications électroniques, en ce compris l'origine et la destination de la communication, la localisation de l'équipement terminal lors de la communication et les métadonnées des appels infructueux, ne peut être généralisée. Elle peut néanmoins opérer, pour une durée limitée au strict nécessaire, de manière ciblée et déterminée par un critère géographique.

L'article 126/1 de la loi du 13 juin 2005 tel que modifié par le projet de loi prévoit que l'obligation de collecte des données dans certaines zones géographiques soit déterminée par des taux relatifs à la criminalité grave qui y sévit. Ainsi, certaines zones considérées comme soumises à un risque élevé de criminalité grave, telles que les aéroports, gares, etc… font l'objet d'une conservation systématique des données des utilisateurs et utilisatrices qui y circulent. Quant aux zones de police ou arrondissements judiciaires sujets à un taux important d'infractions graves, celles-ci font l'objet d'une moyenne sur trois ans par mille habitants. La durée de conservation des données (6, 9 ou 12 mois) varie en fonction du nombre moyen d'infractions constatées.

Tout d'abord, le constat d'infractions se base sur les statistiques de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police (ci-après BNG) et se réfère à la qualification des faits au début de l'enquête pénale. Cependant, il est courant que la qualification première d'une infraction soit modifiée par le parquet en cours d'enquête. Elle n'est donc que provisoire. De plus, le rapport d'activité de relève l'Organe de contrôle de l'information policière (ci-après COC) relève lui-même les nombreuses erreurs, inexactitudes, qualifications erronées données aux faits et encodées dans la BNG[32]. L'utilisation de la BNG comme référence statistique ne peut dès lors être retenue pour justifier l'atteinte aux droits d'un nombre de personnes aussi élevé.

Concrètement, la notion d'infractions graves renvoie à l'article 90ter du Code d'instruction criminelle qui prévoit les cas dans lesquels un·e juge d'instruction peut, à l'aide de moyens techniques, intercepter, prendre connaissance, explorer et enregistrer des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci. L'article précise que « cette mesure ne peut être ordonnée que dans des cas exceptionnels, lorsque les nécessités de l'instruction l'exigent, s'il existe des indices sérieux que cela concerne une infraction visée au paragraphe 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité ». Le caractère exceptionnel et

[32] C.O.C., *Rapport d'activité 2020*, p. 18, disponible sur https://www.organedecontrole.be/files/Rapport-dactivit%C3%A9_COC_2020_F.pdf.

subsidiaire de cette méthode ne fait aucun doute. Cette possibilité est réservée au juge d'instruction et aucune autre autorité.

De plus, la n**otion d'infractions graves** telles que délimitées par l'article 90ter du Code d'instruction criminelle est trop large. Elle comprend notamment des infractions de droit commun telles que le faux informatique, la fraude informatique, le vol avec violence, la détention de stupéfiants et rassemble des infractions susceptibles d'encourir des peines de seuils différents de sorte que la gravité ne semble pas objectivée.

Aucune distinction n'est faite entre la récolte de l'une ou l'autre des métadonnées concernées par le l'avant-projet de loi et les objectifs de défense de la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales. Rompant avec son caractère spécifique originaire, la mesure deviendrait ainsi une méthode générale de poursuite d'une grande majorité d'infractions, ce qui n'apparaît pas proportionnel aux violations des droits qu'elle engendre.

Une observation similaire peut être faite à l'égard des **durées de conservation des données**. La manière dont est menée l'instruction judiciaire relative à l'un ou l'autre type d'infraction devrait permettre de justifier les durées de conservations projetées. A contrario, il conviendrait de démontrer en quoi des durées de conservation plus courtes et moins attentatoires ne permettraient pas la résolution de certains types d'infraction.

Les **taux et leurs seuils** ne sont déterminés par aucun critère objectif. Ils sont explicités et imposés sans aucune justification quant à la nécessité et la proportionnalité de ces choix. En réalité, cette disposition trahit la volonté assumée du législateur de parvenir à une surveillance de masse indiscriminée par le biais de mécanismes hautement attentatoires aux libertés individuelles et ne permettant pas la distinction entre des mesures de conservation minimales et ciblées autorisées par le droit européen dans le cadre d'une politique criminelle de lutte contre la criminalité grave et des mesures spéciales nécessaires dans le cadre d'un état d'urgence criminelle.

Enfin, en plus des fournisseurs de services de communication par téléphone et d'Internet, les services « over the top » (ci-après OTT) tels que les messageries WhatsApp, Skype, Signal ou Facebook sont soumis aux mêmes obligations que les opérateurs télécoms historiques. L'application du critère géographique est susceptible d'entraîner une obligation de collecte des données traitées indistinctement sur l'ensemble du territoire belge par ces services à défaut de pouvoir déterminer la localisation des utilisateurs. Respecter la législation nationale irait à l'encontre de ce que permet la CJUE.

Dès lors, sauf à démontrer l'état d'urgence criminelle - ou à tenter de le normaliser-, rien n'indique que l'évaluation par taux telle que proposée serait justifiée. Sous couvert d'établir un système différencié par zones géographiques reposant sur une évaluation graduée de la criminalité, le projet de loi opère concrètement une couverture généralisée du territoire. En effet, les seuils sont à ce point bas pour couvrir la région bruxelloise et pour supposer qu'ils seront atteints dans toutes les villes et communes du pays.

En outre, le projet de loi prévoit la collecte de ces métadonnées dans des lieux "particulièrement exposés à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave". Au niveau de la proportionnalité, la CJUE n'admet que cela ne soit le cas que dans des "des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages". Vu le nombre de lieux listés par l'article 126/1, §3, 3°,

nous nous rallions à l'opinion du Prof. Dr. iur. Vilenas Vadapalas selon lequel "Reference to „infrastructure sites, transport hubs, areas with above average crime rates or that may be a target for serious crime or are high security risk e.g. affluent neighbourhoods, places of worship, schools, cultural and sports venues, political gatherings and international summits, houses of parliament, law courts, shopping malls, etc." looks like an extensive enumeration of all possible areas and places and doesn't help much in targeting the data retention measure"[33]. En effet, les mesures imposant une conservation ciblée des données à des fins de lutte contre la criminalité grave ne sauraient dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances la justifiant. Le nombre de lieux sélectionnés aboutit à réintroduire, de facto, une obligation de conservation indifférenciée des données d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique.

c. Le cryptage

L'article 127/5, §3 prévoit que "Le recours à la cryptographie, utilisé par un opérateur, visant à garantir la sécurité des communications, ne peut pas empêcher l'exécution d'une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et localiser des communications non accessibles au public". Le § 4 du même article indique que "L'utilisation de la cryptographie par un opérateur étranger, dont l'utilisateur final ou l'abonné est situé sur le territoire belge, ne peut pas empêcher l'exécution d'une demande d'une autorité compétente telle que visée aux paragraphes 2 à 3".

La suppression des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que la conservation des données d'identification, de trafic ou de localisation constitue une ingérence disproportionnée dans le droit au respect de la vie privée des personnes concernées et qui excède dès lors ce qui est nécessaire dans une société démocratique. En outre, comme le mentionne l'APD dans son avis, ces dispositions imposent *de facto* l'insertion de « portes dérobées » (« backdoors ») dans les systèmes de cryptographie afin de pouvoir déchiffrer les messages cryptés. Or, comme l'APD, le relève, il existe un consensus fort dans la communauté scientifique pour considérer que l'insertion de « portes dérobées » (« backdoors ») dans les systèmes de cryptographie présente plus de risques pour la vie privée des personnes concernées et les intérêts supérieurs des Etats que d'avantages en termes de lutte contre la criminalité grave. En ce sens, le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression des Nations Unies a rappelé que les Etats devraient « éviter toutes les mesures qui affaiblissent la sécurité en ligne des individus, telles que des portes dérobées, de faibles standards de cryptographie ou la rétention de clés de chiffrement ». Nous insistons pour que soient supprimées les dérogations au principe selon lequel « l'emploi de la cryptographie est libre ».

***

[33] Traduction libre : La référence aux "sites d'infrastructure, aux nœuds de transport, aux zones présentant un taux de criminalité supérieur à la moyenne ou susceptibles d'être la cible d'infractions graves ou présentant un risque élevé pour la sécurité, par exemple les quartiers riches, les lieux de culte, les écoles, les sites culturels et sportifs, les rassemblements politiques et les sommets internationaux, les parlements, les tribunaux, les centres commerciaux, etc.

IV. Conclusion

La conservation des métadonnées de communication est donc une technique controversée. Alors que les tentatives d'instauration de ce mécanisme se multiplient, les décisions de justice européenne visent à éviter une collecte massive et indiscriminée de données à caractère personnel. Le droit communautaire s'oppose à une législation nationale qui oblige les opérateurs de télécommunication à conserver les données de tous les utilisateurs, sans distinction. L'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. Les exceptions doivent être limitées au strict nécessaire et déroger à l'interdiction de la surveillance généralisée ne peut se faire qu'en cas de menace grave pour la sécurité nationale, à certaines conditions rappelées plus haut, mais consacre le principe de la fin de l'obligation de conservation systématique et indifférenciée de ces données à des fins de lutte contre la criminalité grave. En tout état de cause, la criminalité, même particulièrement grave, ne peut être assimilée à une menace pour la sécurité nationale.

L'annulation de la loi du 29 mars 2016 qui reposait dans son principe même sur une obligation de conservation généralisée et indifférenciée de l'ensemble des données traduit ce raisonnement et impose un changement de perspective que le projet de loi soumis à l'examen ne semble pas vouloir opérer : la conservation des métadonnées doit rester l'exception et les mesures visées doivent assurer, par des règles claires et précises, que la conservation des données est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

Au regard des lacunes dont il a été fait état dans cet avis, aller à l'encontre de ces décisions serait un choix politique désastreux trahissant la volonté assumée du législateur de parvenir à une surveillance de masse indiscriminée par le biais de mécanismes hautement attentatoires aux libertés individuelles. La disproportion entre ces atteintes et les objectifs poursuivis est manifeste et le projet de loi ne permet aucunement de distinguer en quoi la récolte de l'une ou l'autre des métadonnées concernées servirait de manière effective les objectifs de défense de la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales, pas plus qu'elle ne permet la distinction entre des mesures de conservation minimales et ciblées autorisées par le droit européen dans le cadre d'une politique criminelle de lutte contre la criminalité grave et des mesures spéciales nécessaires dans le cadre d'un état d'urgence criminelle. Rompant avec son caractère spécifique originaire, la mesure devient ainsi une méthode générale de poursuite d'une grande majorité d'infractions, ce qui n'apparaît pas proportionnel aux violations des droits qu'elle engendre et excède dès lors ce qui est nécessaire dans une société démocratique.

Il importe de ne pas délibérément attenter à la confiance des citoyen·ne·s et de ne pas chercher à pallier le sous-financement de la justice par l'instauration de méthodes reposant sur une forme de contrôle social de masse et de présomption de culpabilité des individus.