



LIGA VOOR  
MENSENRECHTEN



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).

Date de publication : 15/02/2016

URL : [http://nurpa.be/files/20160215\\_avis-associations-droits-homme-projet-loi-conservation-donnees.pdf](http://nurpa.be/files/20160215_avis-associations-droits-homme-projet-loi-conservation-donnees.pdf)

# Résumé analytique

1. Le Gouvernement ne fournit aucune donnée permettant de démontrer la nécessité de la conservation des métadonnées de communication. Il existe par ailleurs au moins deux études scientifiques distinctes qui concluent à l'absence d'effet de la conservation des métadonnées de communication sur les taux d'élucidation des crimes ;
2. L'analyse des métadonnées de communication révèle des informations intimes, les métadonnées de communication sont privées par nature ;
3. La conservation des métadonnées de communication constitue de la surveillance de masse ;
4. En renversant la charge de la preuve, la conservation des métadonnées de communication crée un contexte de présomption de culpabilité pour l'ensemble des citoyens.

Datapanik, la Liga voor Mensenrechten, la Ligue des droits de l'Homme et la NURPA suggèrent :

1. que le Parlement s'oppose au projet de loi dans son ensemble ;
2. la commande d'une étude indépendante visant à déterminer la nécessité de la conservation des données ;
3. la commande d'une étude indépendante visant à dresser une cartographie des informations actuellement collectées et conservées par les fournisseurs de services de communication au public. L'étude devra s'intéresser notamment à la nature des informations conservées, les durées de conservation effectives, l'exploitation qui en est réalisée, les moyens techniques mis en œuvre pour les protéger, les finalités justifiant leur collecte.

# Sommaire

Résumé analytique.....	2
Sommaire.....	3
Introduction.....	4
Vocabulaire.....	4
Contexte.....	5
La conservation des données, pourquoi ?.....	5
Exposé des motifs du projet de loi.....	6
Absence de démonstration de la nécessité de la conservation des données.....	6
Échec à reconnaître la nature privée des métadonnées de communication.....	7
Collecter tout... la stratégie de l'aiguille dans la botte de foin.....	8
De la présomption d'innocence à la présomption de culpabilité.....	9
La conservation des données constitue de la surveillance de masse.....	10
Le citoyen n'a pas renoncé à sa vie privée.....	10
Conservation à des fins de marketing.....	10
Facebook et le « cloud ».....	11
Stopdataretention.be.....	11
Annexes.....	12
Contexte détaillé.....	12

# Introduction

Le Parlement examine actuellement un nouveau projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques <sup>1</sup>. Ce projet de loi fait suite à l'annulation par la Cour constitutionnelle <sup>2</sup>, l'année dernière, de la loi du 30 juillet 2013 (dite « loi sur la conservation des données ») transposant la directive européenne 2006/24/CE (ci-après « la directive ») <sup>3</sup>, elle-même précédemment invalidée par la Cour de justice de l'Union européenne <sup>4</sup>.

Considérant la volonté manifeste du Gouvernement de précipiter — une fois encore — l'adoption de mesures contraignant les opérateurs de communication à conserver les métadonnées des communications de tous les citoyens belges, il nous semble primordial de déconstruire, une fois pour toutes, les thèses que porte ce nouveau projet de loi et ses variantes sibyllines passées ou à venir.

## Vocabulaire

Les **métadonnées** correspondent à l'ensemble des informations relatives à une communication, à l'exception de son contenu. Si le contenu d'une communication correspond à ce que nous disons, les métadonnées de communication correspondent à ce que nous faisons : qui contacte qui, à quelle heure, pendant combien de temps, depuis quel dispositif, depuis quel endroit, etc.

Par simplification, nous utiliserons systématiquement le terme « **conservation des données** » en lieu et place de « collecte massive et indiscriminée et conservation des métadonnées des communications électroniques ».

- 
- 1 Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques, Chambre des représentants de Belgique, DOC 54 1567/001, <http://www.lachambre.be/FLWB/PDF/54/1567/54K1567001.pdf>
  - 2 « La Cour constitutionnelle annule la loi sur la conservation des données de communication », NURPA, <http://nurpa.be/actualites/2015/06/cour-const-annule-data-retention-belgique>
  - 3 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, page 54, <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32006L0024&from=FR>
  - 4 « La directive sur la conservation des données invalidée par la CJUE », NURPA, <http://nurpa.be/actualites/2014/04/directive-data-retention-invalidée>

# Contexte

*Nota : nous renvoyons le lecteur au titre « Contexte détaillé » dans les annexes pour un exposé plus complet sur ce thème.*

L'adoption de la directive s'est déroulée dans un contexte émotionnel fort, près de deux ans jour pour jour après les attentats de Madrid (quelques mois après les attentats de Londres). Alors que l'idée d'une obligation de conservation des données n'était jamais parvenue à rassembler une majorité, la directive est adoptée en quelques mois seulement.

Dès mars 2010, la Cour constitutionnelle allemande invalide une loi transposant la directive au motif de son incompatibilité avec le droit à la vie privée. Le premier rapport d'évaluation de la Commission échoue à démontrer la nécessité de la conservation des données. En 2012, deux juridictions nationales interrogent la Cour de justice de l'Union européenne (CJUE) sur la compatibilité de la directive avec la Charte des droits fondamentaux.

En Belgique, en juillet 2013, dans ce contexte, alors que le délai de transposition pour la directive est dépassé de plus de quatre ans et qu'aucun des États membres accusant un retard similaire ne s'est vu imposer de sanctions, le Parlement vote — dans le cadre d'une procédure d'urgence requise par le Gouvernement (quelle urgence ?) — le projet de loi transposant la directive.

En juin 2015, la Cour constitutionnelle belge annule cette même loi.

## La conservation des données, pourquoi ?

- Pourquoi une conservation des données plutôt que d'autres mesures ? Quelles autres mesures ont été envisagées ?
- Quels sont les éléments objectifs qui laissaient augurer, à l'époque, que la conservation des données permettrait de lutter contre la criminalité organisée et le terrorisme ?
- Quels sont les éléments objectifs qui démontrent, aujourd'hui (dix ans après l'adoption de la directive), la nécessité et l'éventuelle efficacité de la conservation des données ?
- Quel est l'état des choses en matière de collecte de données par les opérateurs ? Au-delà des obligations de collecte et de conservation, que collectent-ils volontairement (notamment à des fins de marketing), pendant combien de temps ces informations sont-elles conservées ?

Voilà les questions que les membres du Parlement fédéral devraient se poser avant de se précipiter à nouveau, dans un contexte émotionnel particulier, pour adopter un projet de loi substantiellement similaire à celui annulé par la Cour constitutionnelle belge (et tant d'autres à travers l'Europe) il y a quelques mois à peine.

# Exposé des motifs du projet de loi

Dans l'exposé des motifs de son nouveau projet de loi, le Gouvernement fait l'impasse sur ces questions. La conservation des données est présentée comme une solution sans que rien ne vienne jamais étayer le propos.

## Absence de démonstration de la nécessité de la conservation des données

Le point 3 (p. 5), intitulé « *L'importance des données de communication pour les enquêtes pénales et de renseignement* », est vide de toute substance.

Le gouvernement affirme que :

*« les données relatives aux communications jouent un rôle croissant dans les enquêtes pénales et de renseignement. » (p. 5, point 3, § 1)*

Où sont les chiffres qui l'attestent ? Combien de cas cela concerne-t-il ? Dans combien de cas le recours aux données conservées était-il le seul moyen raisonnable d'obtenir les informations désirées ? Dans combien de cas l'absence de ces données a-t-elle, de façon avérée, porté préjudice à une procédure ?

*« Le besoin d'identifier le titulaire d'un numéro de gsm ou d'une adresse IP est devenu un aspect routinier des enquêtes et une étape indispensable de celles-ci. » (p. 5, point 3, § 4)*

Nul besoin de conserver les métadonnées de communication pour parvenir à identifier le titulaire d'un numéro de téléphone ou d'une adresse IP. Les fournisseurs de services de communication sont déjà contraints d'être en mesure d'identifier leurs usagers.

*« L'accès à l'historique des communications ou la localisation a posteriori du suspect ou de la victime sont des mesures plus attentatoires à la vie privée et moins utilisées que l'identification mais sont néanmoins très souvent indispensables dans certains types d'affaires. » (p. 5, point 3, § 4)*

À quel pourcentage cette « moindre utilisation » et ce « très souvent » correspondent-ils ? Combien de cas cela concerne-t-il ?

En fait, les rares études sur le sujet vont à contre-courant des thèses défendues par le Gouvernement :

- 2011, étude commandée par le Bundestag <sup>5</sup> : la conservation des données n'a pas d'effet sur le taux d'élucidation des crimes ;

---

5 (DE) « Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedsstaaten », Johannes Becher, [http://www.vorratsdatenspeicherung.de/images/Sachstand\\_036-11.pdf](http://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.pdf)

- 2012, étude du département de criminologie de l'Institut Max-Planck de droit pénal étranger et international <sup>6</sup> : la conservation des données n'a pas d'effet sur la sécurité des citoyens ; la conservation des données n'a pas d'effet sur le taux d'élucidations des crimes graves ; la conservation des données n'a pas d'effet sur l'élucidation des crimes commis par Internet ; ...

## Échec à reconnaître la nature privée des métadonnées de communication

Le Gouvernement rappelle à trois reprises sur l'espace de huit pages que le contenu des communications n'est pas visé (p. 4, point 1, § 2 ; p. 5, point 3, § 5 ; p. 12, point 7c, § 3). Il tente ainsi de créer une hiérarchie de privacité pour les données potentiellement collectables (voir aussi p. 13, point 8).

Le contenu des communications représenterait l'inébranlable sommet de cette hiérarchie, le reste serait plus légitimement collectable car représentant une intrusion moins importante dans la vie privée des citoyens. Cette thèse est erronée et trompeuse.

Il suffit de s'intéresser à l'anatomie d'un SMS pour le comprendre.

Contenu	
Ça ne va pas mieux.	
Métadonnées	
Heure et date d'envoi	1er janvier 2016, 06h00
Numéro émetteur	0496123456 (facturation : Alice Dubois – 149/1, rue du Midi, Bruxelles)
Localisation émetteur	antenne XYZ987 (située sur le toit de l'hôpital Érasme, Bruxelles)
Id de la carte SIM émetteur	123...
Id du téléphone émetteur	987...
Numéro du destinataire	0487325476 (facturation : Bob Dupont – 149/1, rue du Midi, Bruxelles)
Localisation destinataire	Antenne IJK123 (située devant la gare de Bruxelles-Midi)
Id de la carte SIM destinataire	456...
Id du téléphone destinataire	786...

Tableau 1: anatomie d'un SMS

Qu'est-ce qui révèle plus d'informations, le contenu du message ou le reste (les métadonnées) ?

6 (DE) « Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten », Max-Planck-Institut, <https://www.mpicc.de/de/forschung/forschungsarbeit/kriminologie/vorratsdatenspeicherung.html>

Imaginez, encore, Charlie qui contacte un centre d'information sur le SIDA, puis son médecin, puis ses parents et enfin sa compagne/son compagnon (il est possible de déterminer aisément qui est la compagne/le compagnon de Charlie en observant la fréquence des communications). Est-il nécessaire de connaître le contenu de la conversation pour déterminer l'objet probable des appels ?

Imaginez encore mille autres situations. Les métadonnées de communication révèlent souvent plus d'informations privées que le contenu des communications. Cela ne revient pas à dire qu'elles sont plus privées que le contenu d'une communication mais qu'elles sont privées au même titre, par nature.

*« Les [métadonnées de communication] ne sont pas des données personnelles au sens classique du terme, se rapportant à des informations ponctuelles sur l'identité des personnes, mais des données personnelles pour ainsi dire qualifiées, dont l'exploitation peut permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée. », point 74 des conclusions de Maître Cruz Villalón, avocat général de la CJUE dans le cadre des procédures évoquées plus haut.*

En 2005, un papier issu du Massachusetts Institute of Technology (MIT) <sup>7</sup> met en lumière le fait que les métadonnées de communication révèlent l'identité des collègues, des amis et connaissances d'une personne dans 90% des cas. Elles peuvent également être utilisées pour prédire si deux personnes se réuniront dans les prochaines 12 heures dans 90% des cas. Les données générées par une personne au cours d'une période d'un mois peuvent être utilisées pour prédire où la personne sera dans les prochaines 12 heures dans 95% des cas. Enfin, les données peuvent être utilisées pour prédire l'activité d'une personne au cours des 12 heures suivantes dans 80% des cas.

Voir encore le projet « Pathways » de Mimi Onuoha <sup>8</sup>, chercheuse et artiste qui, à travers différents ensembles de métadonnées, interprète visuellement des morceaux de vie.

Voir aussi « Tell-all telephone » <sup>9</sup>, six mois de métadonnées d'un député allemand croisées avec les informations publiquement disponibles à son sujet (blog, Twitter,...) et présentées sur une carte interactive.

## **Collecter tout... la stratégie de l'aiguille dans la botte de foin**

*« Le secteur du terrorisme est évidemment particulièrement d'actualité. L'accès aux données de communication est une étape incontournable pour identifier les personnes et les liens entre celles-ci. » (p. 5, point 3, § 6)*

L'exemple américain le démontre, la collecte massive et indiscriminée de données ne fonctionne pas pour lutter contre le terrorisme <sup>10</sup>.

7 (EN) « Reality mining: sensing complex social systems », Nathan Eagle, Alex (Sandy) Pentland, Journal « Personal and Ubiquitous Computing », Volume 10, Issue 4, March 2006, Pages 255 – 268, <http://realitycommons.media.mit.edu/download.php?file=realitymining.pdf>

8 (EN) <http://www.nationalgeographic.com/pathways/>

9 (EN) <http://www.zeit.de/datenschutz/malte-spitz-data-retention>, Zeit Online

10 (EN) « Do NSA's Bulk Surveillance Programs Stop Terrorists? », Peter Bergen, David Serman, Emily Schneider and Bailey Cahall, National Security Program, Janvier 2014, [https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS\\_NSA\\_surveillance.pdf](https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf)



Les terroristes connaissent les méthodes des enquêteurs. Depuis des années (avant les attentats du 11 septembre 2001) ils mettent en œuvre des techniques consistant à brouiller les pistes en échangeant les cartes SIM, les mélangeant, voir en évitant tout simplement d'utiliser des moyens de communications qui peuvent laisser des traces ou être interceptés.

Paradoxalement, le texte évoque : « [...] lorsqu'une perquisition mène à la découverte d'un sac entier de cartes SIM [...], il s'ensuit un grand nombre d'actes d'enquêtes pour retracer les communications passées à partir de ces éléments [...] » (p. 6, § 1) mais échoue une fois de plus à fournir des données sur les cas dans lesquels l'analyse de ces « sacs de cartes SIM » en utilisant les métadonnées conservées par les opérateurs conduit à quoi que ce soit de pertinent.

Dans le cadre d'enquêtes visant des faits de terrorismes, les enquêteurs disposent d'outils juridiques permettant la mise sur écoute ciblée et la collecte d'informations. Il est tout à fait salubre d'être en mesure d'opérer de la surveillance ciblée lorsque celle-ci se fonde sur des éléments concrets et est encadrée par un juge.

Terrorisme, pédophilie, piratage, faux médicaments sont autant de thèmes graves et chargés en émotions que le Gouvernement évoque sans jamais fournir de données concrètes. Le passage suivant est particulièrement révélateur :

*« [...] La réalité est que les données de communications sont nécessaires dans une grande variété de situations mais où on imagine aisément que ces données sont souvent à la fois le point de départ et une étape de l'enquête [...] » (p. 6, §3)*

Nous espérons que le Gouvernement ne s'est pas contenté d'« imaginer » des cas d'usages hypothétiques et a rassemblé une série de données permettant de soutenir ces affirmations (et toutes les autres présentes dans l'exposé des motifs).

## **De la présomption d'innocence à la présomption de culpabilité**

Le Gouvernement tente de légitimer son projet de loi en indiquant que la conservation des données peut « [...] jouer à charge comme à décharge. » (p. 10, point 7, a, § 4).

Le citoyen devrait accepter la conservation des données au motif que cela permettrait potentiellement de fournir des données de nature à le disculper. Cela revient à inverser la charge de la preuve.

## **La conservation des données constitue de la surveillance de masse**

Lorsque le Gouvernement indique verbatim que « *la conservation des données n'est pas de la surveillance de masse* » (p. 7, point 4), il précise dans le même temps qu'« *il ne fait pas de doute que l'obligation de conserver les données de communication constitue une limitation majeure de la vie privée des individus* ».

*« Il est toutefois essentiel de ne pas confondre cette obligation de conservation avec la surveillance de masse réalisée par certains pays [...]. Cette surveillance est caractérisée par le fait que des services étrangers filtrent et traitent effectivement un nombre gigantesque de données. »* (p. 7, point 4, § 2)

*« La mesure visée par le présent projet de loi ne relève pas du tout de ce type d'approche. Si la conservation touche effectivement tous les citoyens pour autant qu'ils utilisent un téléphone ou Internet, l'accès à et l'utilisation de leurs données seront toujours ciblé [...] »* (p. 7, point 4, § 3)

La nuance nous échappe. Elle nous échappe d'autant plus que Maître Cruz Villalón, avocat général de la Cour de justice de l'Union européenne (CJUE), dans son avis dans le cadre des questions préjudicielles sur la directive n'hésitait pas à parler de surveillance :

*« [...] La collecte de ces données crée les conditions d'une surveillance qui, pour ne s'exercer que rétrospectivement à l'occasion de leur exploitation, menace néanmoins de manière permanente, pendant toute la durée de leur conservation, le droit des citoyens de l'Union au secret de leur vie privée. [...] »* point 72 des conclusions de Maître Cruz Villalón, avocat général de la CJUE dans le cadre des procédures évoquées plus haut.

## **Le citoyen n'a pas renoncé à sa vie privée**

Le Gouvernement tente de justifier la collecte massive et indiscriminée et la conservation des métadonnées des communications électroniques par le fait que les citoyens consentent ou soient contraints, en certaines occasions, à ce que leurs données soient conservées.

### **Conservation à des fins de marketing**

*« Il faut néanmoins rappeler que les citoyens, en souscrivant les abonnements de téléphonie ou d'accès à Internet, consentent à ce que les données de communication nécessaires non seulement à la facturation mais aussi au marketing soient conservées par l'opérateur aussi longtemps que cela est nécessaire pour ces finalités. »* (p. 8, point 5, § 2)

S'il est nécessaire que le citoyen consente à ce que ses données soient traitées à des fins de facturation lorsqu'il souscrit à un abonnement de téléphonie ou d'accès à Internet, il n'en est pas de même pour les finalités relatives au marketing. Cependant, dans la vaste majorité des cas, le fournisseur de service s'assure d'obtenir le « consentement » en l'implémentant sous forme d'*opt-out* : le citoyen consent par défaut, il s'agit de l'une des clauses du contrat auquel il doit adhérer en entier pour pouvoir souscrire au service.

On ne peut, dès lors, pas considérer qu'il s'agit d'un consentement explicite et informé.

### **Facebook et le « cloud »**

*« Les citoyens confient par ailleurs de plus en plus de données électroniques parfois extrêmement sensibles à des acteurs privés (Facebook par exemple mais aussi les systèmes de messagerie ou de stockage dans le “cloud”). Ces acteurs privés reçoivent de leurs utilisateurs l'autorisation de traiter de manière continue des données personnelles de plus en plus massives et dont la combinaison permet de savoir énormément de choses sur la personne. » (p. 9, § 2)*

D'emblée, il convient de rappeler au Gouvernement que Facebook est une société privée, pas un État. L'utilisation de Facebook et autres relève du libre choix de chaque citoyen, contrairement au présent projet de loi qui s'imposerait *de facto* à l'ensemble de la population.

Ensuite, l'utilisation de Facebook et autres ne nécessite pas de livrer des informations personnelles.

Enfin, à l'instar de la situation pour la conservation à des fins de marketing, on peut légitimement se questionner sur la nature informée et explicite du consentement concédé par les utilisateurs de ces plate-formes quant à l'exploitation de leurs données.

### **Stopdataretention.be**

À titre anecdotique : l'un des recours à l'origine de l'annulation par la Cour constitutionnelle de la précédente loi sur la conservation des données a été financé par un crowdfunding (dont l'objectif a été dépassé en seulement quelques jours).

# Annexes

## Contexte détaillé

- **11 mars 2004**, deux ans et demi après les attentats du 11 septembre 2001 (USA), des attentats revendiqués par Al-Qaïda frappent l'Espagne <sup>11</sup>.
- **Juillet 2005**, le Royaume-Uni est frappé par des attentats revendiqués par Al-Qaïda <sup>12</sup>.
- **15 mars 2006**, presque deux ans jour pour jour après les attentats de Madrid, le Parlement européen adopte, au terme d'une course effrénée de 3 mois à travers des différentes institutions européennes (ce qui en fait l'une des adoptions les plus rapides de l'histoire de l'Union), la directive 2006/24/CE.

La directive contraint les fournisseurs de services de communication à conserver les métadonnées de communication de l'ensemble de leurs usagers pour une durée allant de six mois à deux ans. Elle vise à harmoniser les législations des États membres afin de lutter contre la criminalité organisée et le terrorisme.

- **Mars 2010**, la Cour constitutionnelle allemande annule la loi nationale transposant la directive <sup>13 14</sup>.
- **Avril 2011**, la Commission européenne présente un rapport d'évaluation de la directive <sup>15</sup>.
- **Septembre 2011**, le Contrôleur européen de la protection des données (autorité de contrôle indépendante au niveau de l'UE) émet un avis sur le rapport d'évaluation de la Commission <sup>16</sup>.

Sur base du rapport, il estime notamment : « *que la directive a failli à son objectif principal, à savoir l'harmonisation des législations nationales* » ; « *que la nécessité de la conservation des données [...] n'a pas été suffisamment démontrée* ». Il appelle par ailleurs la Commission « à envisager sérieusement [...] la possibilité d'abroger purement et simplement la directive ».

---

11 « Attentats de Madrid du 11/03/2004 », [https://fr.wikipedia.org/wiki/Attentats\\_de\\_Madrid\\_du\\_11\\_mars\\_2004](https://fr.wikipedia.org/wiki/Attentats_de_Madrid_du_11_mars_2004)

12 « Attentats de Londres du 07/07/2005 », [https://fr.wikipedia.org/wiki/Attentats\\_du\\_7\\_juillet\\_2005\\_%C3%A0\\_Londres](https://fr.wikipedia.org/wiki/Attentats_du_7_juillet_2005_%C3%A0_Londres)

13 (EN) « Data retention unconstitutional in its present form », communiqué de presse 11/2010 de la Cour constitutionnelle fédérale d'Allemagne, 2 mars 2010, <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html>

14 (EN) Jugement 1 BvR 256/08 de la Cour constitutionnelle fédérale d'Allemagne, 2 mars 2010, [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302\\_1bvr025608en.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html)

15 « Rapport de la Commission au Conseil et au Parlement européen : rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE), COM/2011/0225 final », 18 avril 2011, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:FR:HTML>

16 « Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE), 2011/C 279/01 », Journal officiel de l'Union européenne (ISSN 1725-2431), 23 septembre 2011, page 1, <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52011XX0923%2801%29&qid=1455382995237&from=FR>

- **Juin et septembre 2012**, deux juridictions nationales (Irlande, Autriche) adressent des demandes de décision préjudicielle portant sur la validité de la directive à la Cour de justice de l'Union européenne (CJUE) <sup>17</sup>.
- **Juillet 2013**, le Parlement fédéral adopte, dans le cadre d'une procédure d'urgence, un projet loi transposant la directive en droit belge <sup>18</sup>.
- **Décembre 2013**, Maître Cruz Villalón, avocat général de la CJUE remet son avis dans le cadre des questions préjudicielles soulevées par les juridictions autrichienne et irlandaise <sup>19</sup>.

Il conclut à l'incompatibilité de l'ensemble de la directive avec [...] la charte des droits fondamentaux de l'Union européenne.

- **Février 2014**, la NURPA, Datapanik, la Liga voor Mensenrechten et la Ligue des droits de l'Homme initient conjointement une campagne de crowdfunding <sup>20</sup> pour financer une procédure de recours auprès de la Cour constitutionnelle afin d'obtenir l'annulation de la loi sur la conservation des données.

Deux recours en annulation sont introduits indépendamment, l'un par ces associations, l'autre par l'Ordre des barreaux francophones et germanophones.

- **Avril 2014**, la CJUE, dans le cadre des demandes de décision préjudicielle soulevées par les juridictions autrichienne et irlandaise, invalide la directive <sup>21</sup>.
- **Juin 2014**, la Cour constitutionnelle autrichienne annule la loi nationale transposant la directive <sup>22</sup>.

17 Affaires jointes (C-293/12 et C-594/12) Digital Rights Ireland et Seitlinger e.a., InfoCuria, <http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=fr>

18 « 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 », Moniteur belge du 23 août 2013, pages 56109 à 56112, [http://www.ejustice.just.fgov.be/mopdf/2013/08/23\\_1.pdf#Page7](http://www.ejustice.just.fgov.be/mopdf/2013/08/23_1.pdf#Page7)

19 « Conclusions de l'avocat général M. Pedro Cruz Villalón sur les affaires C-293/12 et C-594/12 », Cour de justice de l'Union européenne, 12 décembre 2013, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1>

20 <http://stopdataretention.be>

21 « Arrêt de la cour (grande chambre) du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 », Cour de justice de l'Union européenne, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=167431>

22 (DE) « Die Vorratsdatenspeicherung ist Geschichte! », Arbeitskreis Vorratsdaten Österreich, 27 juin 2014, <https://www.akvorrat.at/die-vorratsdatenspeicherung-ist-geschichte>

- **Juillet 2014**, la Cour constitutionnelle slovène annule la transposition nationale de la directive et impose la destruction de toutes les données collectées <sup>23 24</sup>.

Quelques jours plus tard, la Cour constitutionnelle roumaine annule, pour la seconde fois, la loi nationale transposant la directive <sup>25</sup>.

- **Mars 2015**, le tribunal du district de La Haye invalide la loi néerlandaise transposant la directive <sup>26</sup>.

Quelques jours plus tard, la Cour constitutionnelle bulgare annule à son tour la loi nationale transposant la directive <sup>27</sup>.

- **Avril 2015**, la Cour constitutionnelle slovaque annule la loi nationale transposant la directive <sup>28 29</sup>.

- **Juin 2015**, la Cour constitutionnelle belge annule la loi sur la conservation des données transposant la directive <sup>30</sup>.

---

23 (EN) « Slovenia : Data retention unconstitutional, deletion of data ordered », European Digital Rights, 16 juillet 2014, <https://edri.org/slovenia-data-retention-unconstitutional/>

24 (SL) Décision U-I-65/13-19 de la Cour constitutionnelle slovène, 3 juillet 2014, [https://www.ip-rs.si/fileadmin/user\\_upload/Pdf/sodbe/US\\_RS\\_ZEKom-1\\_3julij2014.tif](https://www.ip-rs.si/fileadmin/user_upload/Pdf/sodbe/US_RS_ZEKom-1_3julij2014.tif)

25 (RO) Communiqué de presse de la Cour constitutionnelle de Roumanie, 8 juillet 2014, <http://www.ccr.ro/comunicate/COMUNICAT-DE-PRES-346>

26 (NL) Arrêt invalidant la loi, 11 mars 2015, <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498>

27 (EN) « Bulgaria's Constitutional Court scraps data retention provisions », The Sofia Globe, 12 mars 2015, <http://sofiaglobe.com/2015/03/12/bulgarias-constitutional-court-scraps-data-retention-provisions/>

28 (EN) « The Slovak Constitutional Court cancelled mass surveillance of citizens », European Information Society Institute, 29 avril 2015, <http://www.eisionline.org/index.php/sk/projekty-m-2/ochrana-sukromia/109-the-slovak-constitutional-court-cancelled-mass-surveillance-of-citizens>

29 (SK) Arrêt PL. ÚS 10/2014-78 de la Cour constitutionnelle slovaque, 29 avril 2015, [http://www.eisionline.org/images/Data\\_retention\\_rozhodnutie\\_PL\\_US\\_10\\_2014.pdf](http://www.eisionline.org/images/Data_retention_rozhodnutie_PL_US_10_2014.pdf)

30 Arrêt 84/2015 de la Cour constitutionnelle, 11 juin 2015, <http://www.const-court.be/public/f/2015/2015-084f.pdf>