Chers députés,

Vous discutez en ce moment d'un sujet cher à mon cœur et sur lequel je travaille depuis des années au niveau allemand et européen : la conservation des données.

Je suis un député européen pour le parti Pirate, et docteur en droit. Avant d'être juge puis eurodéputé, j'ai fait mon doctorat sur le sujet de la conservation des données. Mon travail a contribué à l'annulation de la loi allemande devant la Cour Constitutionnelle. Ainsi, j'ai toujours observé avec intérêt les développements en la matière dans les différents États Membres.

Suivant plusieurs arrêts de la Cour de Justice Européenne (CJUE), beaucoup d'États Membres cherchent comment rétablir des régimes de surveillance de masse pourtant invalidés maintes fois, sans concession pour les valeurs démocratiques ou le droit à la vie privée – la surveillance à tout prix. Dans ce cadre, la Belgique pourrait établir un précédent dangereux pour les autres États Membres, et c'est pourquoi je voudrais pointer du doigt, tant qu'il est encore temps, quelques failles de taille qui, si elles ne sont pas adressées maintenant, conduiront potentiellement à l'annulation de la loi devant la Cour. De plus, je noterais que la Commission Européenne est en train de regarder pour une solution européenne – faire avancer les choses au niveau national n'a pas tout son sens au moment présent.

Permettez donc que j'intercède, en tant que citoyen concerné, en tant qu'expert en la matière, et en tant que votre homologue au niveau européen. Je vous soumets le présent avis, d'initiative propre, en espérant que vous ayez l'opportunité de me lire avant de voter sur le projet de loi.

<u>En résumé :</u>

A travers ce projet de loi, le gouvernement recherche la connaissance d'informations à n'importe quel prix, et de ce fait ne respecte que très mal – sans doute sciemment – l'esprit de la jurisprudence en la matière ainsi que les droits fondamentaux. La surveillance redeviendrait la norme plutôt que l'exception ; un changement radical est nécessaire, beaucoup plus basée sur le *quick* et *future freeze*, sur un meilleur investissement dans les ressources des services de police, de renseignement et juridiques, et dans des méthodes plus ciblées pour certains crimes graves spécifiques.

Sur les éléments du projet de loi :

- Période de conservation obligatoire pour combattre la fraude:
  - Comme une conservation de données indiscriminée n'est pas justifiée pour résoudre des crimes graves, il est clair que combattre la fraude ne la justifie pas non plus.
  - Autres problèmes: la conservation *obligatoire*; la dérogation *générale* au principe de confidentialité; les catégories de données *supplémentaires*; le recours à, et la justification basée sur le *futur* Règlement ePrivacy, qui préempte les négociations du Parlement Européen.
- Conservation des données 'ciblée' en fonction d'un taux de criminalité grave :
  - la CJUE permet la conservation ciblée « étant entendu qu'il ne saurait être question de réinstaurer, par ce biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation .» Vu les modalités choisies, le projet de loi couvrira cependant la totalité du territoire et de la population, rétablissant *de facto* cette surveillance généralisée.

- Lorsque la CJUE fait référence à une incidence élevée de la criminalité grave, le terme "élevée" implique qu'elle doit être plus que légèrement supérieure à la moyenne, vu que la conservation des données est une mesure d'exception.

- Conservation des données ciblée visant des bâtiments importants, stratégiques, vitaux et autres :
  - Seuls les sites qui "reçoivent régulièrement un très grand nombre de visiteurs" et qui sont "particulièrement vulnérables à la commission d'infractions pénales graves" peuvent être couverts. Lister dans la loi tous les sites où transitent en Belgique beaucoup d'individus (tel que l'entièreté du réseau autoroutier), ne constitue pas un tel ciblage.
- Conservation des données ciblée visant des bâtiments des Institutions Internationales :
  - Si la rétention de données constitue une grave menace pour la démocratie au niveau national, je pense également que le processus démocratique européen est menacé si les autorités et les services de renseignement belges sont en mesure d'accéder aux données de localisation, de trafic et de communication des députés européens et de tous les individus qui mettent les pieds dans le périmètre entourant le Parlement. Cet argument est valable aussi pour les autres institutions internationales, qui devraient être consultées avant de se voir imposer cette 'protection'.
- Sur la question de couvrir ou non les OTT:
  - Une loi de surveillance couvrant les OTT capturerait tout contact confidentiel dans le privé, le professionnel et le gouvernement.
- Sur la question de l'encryptage
  - La cybersécurité et la confiance envers l'État n'est pas donnée quand on est un activiste, journaliste d'investigation (ou sa source) ou opposant politique (voire avocat, conseiller, victime ayant besoin de l'anonymat) – qui plus est depuis la débâcle Pegasus. Cette conservation des données et son impact sur l'encryptage est un pas de plus affaiblissant cette cybersécurité et cette confiance.
- Les adresses IP et autres données:
  - La conservation indiscriminée des adresses IP et des données d'identification de tous les utilisateurs de services de communication dans l'UE, porte atteinte au droit d'utiliser Internet et de communiquer de façon anonyme.
  - De plus, les nouvelles caractéristiques de l'IPv6 n'avaient pas encore été prises en compte par la Cour quand elle permettait cette conservation des adresses IP, ce qui (à la lumière de l'ingérence accrue causée par l'IPv6) devrait conduire le législateur à la prudence et la nuance quand il la prévoit.

Honorables représentants du peuple belge, la conservation des données est probablement l'instrument de surveillance qui porte le plus atteinte à la vie privée que l'État aie à sa disposition. Elle porte atteinte au secret professionnel, crée un risque permanent de perte et d'abus de données et dissuadera les citoyens de faire part de communications confidentielles via les réseaux de communication électronique. Elle porte atteinte à la protection des sources journalistiques et compromet ainsi la liberté de la presse. Dans l'ensemble, elle porte atteinte aux fondements de notre société ouverte et démocratique. Votez pour défendre le droit à la vie privée et à la liberté de communication !

Je vous prie d'agréer, Mesdames et Messieurs les députés, mes respectueuses et sincères salutations.

Dr Patrick Breyer, député européen

Avec ce projet de loi, il y a un choix politique (celui de la surveillance), ainsi qu'un choix plus juridique (quels moyens et procédures satisfont les règles de la CJUE).

1. Le choix politique:

- Dans une société démocratique (le pouvoir par le peuple), **la surveillance des citoyens** (et plus particulièrement la rétention systématique de leurs données de communications) **doit être l'exception et non la règle.**

- Un des dénominateurs communs des démocraties est l'existence d'institutions et de lois visant à protéger la population des dérives tyranniques ou dictatoriales que peut exercer une personne ou un groupe quelconque, y compris la majorité. Les lois mettant en place une mesure qui *de facto* équivaut à de la surveillance de masse mettent en péril ce fragile équilibre, et amènent le pays toujours plus près du monde dystopique du gouvernement 'Big Brother' de Georges Orwell ou de la Stasi allemande. La Chine et les Etats Unis sont facilement pointés du doigt par le Ministre van Quickenborne, mais **il reste à prouver que le chemin sur lequel s'avance la Belgique avec ce projet de loi est foncièrement différent sur le fond** – surtout qu'une analyse d'impact semble manquer, vu que le Ministre déclarait en commission il y a 2 semaines ne même pas savoir quelle proportion du territoire et de la population sera couvert par les mesure telles qu'entrevues par sa loi.

- 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**.[1] Les demandes de données de communication sont rarement fructueuses, même en l'absence d'une législation sur la conservation des données sans discernement.[2] Le taux d'élucidation de la cybercriminalité en Allemagne, par exemple, est de 58,6 % et se situe au-dessus de la moyenne même sans conservation des données IP. Il avait même chuté lorsque la législation sur la conservation des données a été promulguée (celle-ci a ensuite été invalidée).
- **Aucune autre loi de surveillance n'empiète aussi profondément sur notre vie privée** que la rétention indiscriminée de nos contacts, mouvements et connexions Internet. Il n'existe aucune preuve que la rétention des données de télécommunications permette une meilleure protection contre la criminalité. En revanche, on constate qu'elle coûte des milliards d'euros, qu'elle met en danger la vie privée des innocents, qu'elle perturbe les communications confidentielles et qu'elle ouvre la voie à une accumulation toujours plus massive d'informations sur l'ensemble de la population.

    - Certains pays ont fait le choix politique de ne pas recourir à la conservation des données. La Belgique aussi peut faire ce choix !

2. Le choix juridique

<u>Conservation des données pour combattre la fraude</u>

- La période de conservation obligatoire (des données de localisation) pour combattre la fraude est longue (4 mois[3]), et couvre tous les utilisateurs, sur tout le territoire, tout le temps. Couplé à la possibilité pour les services de renseignement d'accéder aux données conservées

1 Etude: « No statistically relevant effects of data retention ». https://www.patrick-breyer.de/?p=593219
2 Etude: « Traffic data requests rarely unsuccessful even without data retention ». https://www.patrick-breyer.de/?p=594061
3 Etendu à 12 mois si pertinent pour un cas de fraude ou d'utilisation malveillante.

dans cette finalité[4], nous arrivons à une nouvelle forme de surveillance indiscriminée telle que rejetée par la CJUE: Il y a un risque trop élevé que les autorités aient systématiquement recours à cette voie (si cette disposition était la seule forme d'accès), ce qui rétablirait la surveillance de masse. Comme une conservation de données indiscriminée n'est pas justifiée pour résoudre des crimes graves, il est clair que combattre la fraude ne la justifie pas non plus.

- Dans son exposé des motifs (p27), le gouvernement met de côté les recommandations de l'APD sous le prétexte que la conservation réactive ne peut arriver à l 'effet désiré de la conservation préventive. C'est pourtant exactement le même raisonnement que celui avancé pour justifier la conservation généralisée et indiscriminée, rejeté malgré tout par la CJUE. Si ce raisonnement n'est pas acceptable concernant le terrorisme, pourquoi serait-il acceptable concernant la simple fraude ? Non, « les opérateurs ne disposent pas d'une boule de cristal », mais là n'est pas la question.

- Le fait que les utilisateurs de différents fournisseurs auraient des services de qualité différente selon que leur fournisseur utilise ou non la conservation des données pour combattre la fraude et l'utilisation malveillante, ne peut pas justifier de rendre cette **conservation obligatoire** pour tous les opérateurs. Ce serait aberrant comme raisonnement. Comme le souligne l'APD (p675), « la raison pour laquelle il est nécessaire de passer d'une possibilité à une obligation n'apparaît pas suffisamment développée et étayée dans l'Exposé des motifs. » La «**dérogation au principe de confidentialité** » envisagée (p30) est elle aussi disproportionnée ; cette dérogation est trop vague, il faudrait plutôt que l'opérateur puisse déroger seulement sur invitation de l'utilisateur, comme quand celui-ci signale un cas suspect ou un cas clair de fraude. De plus, le gouvernement voudrait permettre la conservation d'encore **plus de catégories** de données (pp30-31, 33) afin de combattre la fraude (avec ou sans arrêt royal), ce qui est non-nécessaire (et de toute façon trop vaguement formulé).

- L'article 9 de la Directive ePrivacy ne prévoit pas le traitement et la conservation des données de localisation autres que les données de trafic qui sont nécessaires pour le bon fonctionnement et la sécurité du réseau ou du service, pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau ou pour répondre à une obligation légale de l'opérateur. Cela peut être permis sous l'article 15 § 1 de la Directive ePrivacy, mais à condition de remplir les conditions de nécessité et proportionnalité, ce qui n'est pas le cas (comme indiqué par l'APD, l'exposé des motifs ne justifie pas cela, v. p678).
  - Pour pallier à cela et requérir le traitement de données supplémentaires, le législateur entre autres se base sur le future Règlement ePrivacy, qui est au stade de trilogue au niveau UE. **Patrick Breyer est shadow rapporteur pour la commission LIBE sur ce dossier. Il rappelle que ce Règlement n'est pas encore adopté, qu'il a déja pris et pourra encore prendre beaucoup de temps avant de l'être, et qu'il pourrait même finir par ne pas être adopté tout court.** Il est anti-démocratique de préempter le processus démocratique au niveau Européen en se basant sur un texte qui est encore au stade des négociations entre le Parlement Européen et le Conseil. (Ce même raisonnement s'applique à la sécurité des réseaux, p37 de l'exposé des motifs).

- Dans le projet de loi, le concept de 'fraude' et de 'sécurité des réseaux' est peut être

4 v. pp159-161 du projet de loi; v. aussi le risque d'abus et d'accès illicite rappelé par la CJUE dans Garda Síochána, §46

différent des concepts utilisés dans ePrivacy.[5] Voyez par exemple pour la sécurité des réseaux le grand écart entre la notion de « défaillance technique ou une erreur dans la transmission des communications » de l'ePrivacy et la "la capacité des réseaux et services de communications électroniques de résister, à un niveau de confiance donné, à toute action qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces réseaux et services, de données stockées, transmises ou traitées » de la directive (UE) 2018/1972. Le harcèlement téléphonique devrait-il être combattu lui aussi par une surveillance de masse ? (dans le cadre de la lutte contre l'utilisation malveillante des réseaux).

Conservation des données 'ciblée' en fonction d'un taux de criminalité grave

- Le gouvernement joue avec les mots dans son interprétation de la CJUE. Vu les modalités choisies par le gouvernement pour enclencher les mesures de conservation des données sur les arrondissements ou zones de police (i.e. les seuils quand aux taux de crimes 90ter par 1000 habitant sur une moyenne de 3 ans), il apparaît que la totalité du territoire et de la population sera couvert, rétablissant *de facto* la surveillance généralisée de l'ancienne loi jugée anticonstitutionelle.[6]

  La CJUE dans son dernier arrêt (Garda Síochána) était pourtant assez claire à ce sujet :

  > §40. « En ce que l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'adopter des mesures législatives visant à « limiter la portée » des droits et des obligations prévus notamment aux articles 5, 6 et 9 de cette directive, tels que ceux découlant des principes de confidentialité des communications et de l'interdiction du stockage des données y afférentes, rappelés au point 35 du présent arrêt, **cette disposition énonce une exception à la règle générale** prévue notamment à ces articles 5, 6 et 9 **et doit ainsi, conformément à une jurisprudence constante, faire l'objet d'une interprétation stricte**. **Une telle disposition ne saurait donc justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications** électroniques et des données y afférentes, et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de ladite directive, **devienne la règle, sauf à vider largement cette dernière disposition de sa portée. »**
  >
  > §65. « […] il importe, dans une société démocratique, que [la conservation des données] soit [...] l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose **même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique** ainsi que de l'importance qu'il convient de leur reconnaître. »
  >
  > §83. « […] c'est [aux États membres] et non à la Cour qu'il incombe d'identifier de tels critères [pour mettre en œuvre une conservation ciblée], **étant entendu qu'il ne saurait être question de réinstaurer, par ce biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.**

La CJUE a statué qu'on ne peut pas surveiller toute une population sans raison valable – mais c'est ce que ferait en réalité cette loi belge. À suivre l'opinion juridique (p34) de l'ancien juge de la CJUE, Prof. Dr. iur. Vadapalas, il est clair que les paramètres suggérés par la Belgique « peuvent conduire à imposer aux fournisseurs des obligations juridiques injustifiées de conserver les données

5 Garda Síochána : « la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs »

6 Le gouvernement semble être pertinemment au courant de ce fait, puisque l'exposé des motifs reconnaît explicitement (p12) « qu'**il n'est pas impossible que l'entièreté du territoire national soit visé par une conservation des données.** Autrement formulé, […] [s]i cette hypothèse est rencontrée, il s'agira alors d'**une conservation ciblée dans son approche mais généralisée dans ses conséquences.**"

relatives au trafic et à la localisation dans des zones géographiques très larges, multiples et indéfinies », ce qui serait contraire à l'idée de ciblage autorisé par la CJUE.

- Il est clair que le taux minimum (v. p62) choisi par le gouvernement a été sélectionné dans un but précis : afin de maintenir le *status quo*, i.e. permettre aux services de police et de renseignements de continuer à accéder aux données de tous les citoyens, comme c'était le cas auparavant. Évidemment, **la CJUE n'a pas donné de critère précis sur la façon de cibler les zones géographiques, mais ce n'est pas une raison pour que le gouvernement fixe des seuils si bas que la conservation soi-disant ciblée n'en soit plus une.** Il est bien difficile d'établir objectivement quel devraient être les seuils, et je ne prétends pas pouvoir répondre à la question ; cependant, le manque de justification et de critère objectif quant au choix de ces seuils[7] fait cruellement défaut au projet de loi, et ne laisse le lecteur que supposer qu'ils ont été choisis pour une raison particulière – celle de couvrir la plus grande partie du territoire possible. Notez que dans son opinion juridique, l'ancien juge de la CJUE Vadapalas, déclare (p31) que **lorsque la CJUE fait référence à une incidence élevée de la criminalité grave, le terme "élevée" implique qu'elle doit être plus que légèrement supérieure à la moyenne**. Quelle est cette moyenne, en Belgique ? Comment s'assurer que la conservation des données restera l'exception ?
  Mais rentrer dans ce débat implique d'accepter la supposition fondamentale derrière ce seuil, qui est que passé un certain taux de criminalité grave, l'entière population de la zone concernée devrait être surveillée – tandis que je pars du principe que ce genre de surveillance ne devrait même pas arriver, et que d'autres moyens devraient être mis en œuvre à la place.

Pour ce qui est de la liste des crimes qui, une fois signalés à la police et reportés dans la banque de donnés BNG, rentrent dans le calcul d'un taux de criminalité grave, il faut noter plusieurs choses.

- Le concept de crime grave n'étant pas défini dans le droit EU ou belge, le gouvernement a repris les crimes pour lesquels un juge peut mandater des écoutes téléphoniques de personnes suspectes (v. raisonnement pp57-59). Cependant, rien ne dit que cette liste de crimes soit pertinente : sont-ils tous graves au point de pouvoir, conjointement, mener à une 'écoute' des données de trafic et de localisation de tous les individus présents dans la zone où ils ont été commis ? J'ai répertorié, dans l'annexe à ce document, les crimes repris sous l'article 90ter. Il ressort de mon analyse les observations suivantes :
  - Ces autorisations d'écoutes téléphoniques par un juge ne concernent à chaque fois qu'une poignée d'individus tout au plus. La conservation des données géo-ciblées du projet de loi, elle, concernerait les milliers de gens passant, travaillant ou vivant dans les arrondissement judiciaire ou zones de police pertinents. **L'ingérence est très différente en terme d'échelle**.[8] La liste des crimes sur lesquels la première ingérence peut être basée ne doit pas forcément être la même que celle de la seconde.
  - La conservation des données est une mesure de surveillance très sérieuse, et doit vraiment être ciblée, ce qui implique peut-être de réduire les catégories de crimes qui peuvent la déclencher. Peu importe que le droit belge pour l'instant les prenne en compte pour ce qui est d'autoriser les écoutes téléphoniques (et autres, v. pp55-56)– cela est une autre histoire. Si le gouvernement veut éviter que la CJUE ait à se pencher sur la question de ce qui peut être qualifié de 'crime grave' (une question plus de la compétence des Etats Membres, mais pas hors de portée de la CJUE), il devrait être plus

7 i.e. pourquoi 3 et pas 10? Qu'est ce qui constitue un seuil suffisant pour surveiller tout le monde dans une zone donnée ? L'exposé des motifs explique le raisonnement du seuil, du pour-mille-habitants, de la durée de conservation croissante etc. pp58-59 mais pas cette question.

8 Mais pas en terme de sensibilité, v. arrêt Garda Síochána §45-47.

restrictif dans la liste des crimes qu'il prend en compte pour déclencher la conservation des données ciblée.
    - Je noterai aussi que l'écoute téléphonique « 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. » C'est bien là tout le contraire en ce qui concerne la conservation des données proposée par le gouvernement : elle sera *de facto* la règle non pas l'exception, et alors qu'il existera bien souvent d'autres moyens d'investigation (moins souvent choisis car plus coûteux, peut être) pour arriver à la vérité.

- La BNG est connue pour ne pas contenir que des données de qualité – cela se sait même au niveau Européen ! Les erreurs et inexactitudes pourraient avoir un impact énorme sur la population. De plus, il y a le problème que ce sont les crimes reportés qui comptent, pas ceux dont on est sûr (via un jugement) qu'ils ont vraiment été commis.

- Le Ministre van Quickenborne déclare que l'option de cibler certaines catégories de personnes est permise par la CJUE mais « trop stigmatisant ». « On pourrait conserver toutes les données de toutes les personnes ayant un casier judiciaire » dit-il, « mais que est le signal que l'on envoie à ces personnes? » Si l'on suit l'esprit de ce raisonnement, cependant, je ne vois pas pourquoi on permettrait de cibler l'entièreté de la population d'un arrondissement judiciaire seulement afin de résoudre quelques crimes graves – **quel est le signal que l'on envoie à ces personnes, si ce n'est que leurs droits fondamentaux peuvent être bafoués et échangés contre un petit peu de sécurité** ? La Belgique n'est pas dans un quelconque 'état d'urgence criminelle' (qui plus est au vu des statistiques de la police qui montrent que la criminalité reste constante, voire décroît) qui justifierait hypothétiquement une quelconque surveillance de sa population, que ce soit dans une zone de police, un arrondissement judiciaire ou *de facto* le territoire entier. (Cette question de l'état d'urgence' a aussi été examinée par l'ancien juge de la CJUE Vadapalas, pour ce qui concerne la loi récente en France. Sa réponse (p22) : la Décision du Conseil d'État n'est pas conforme à la jurisprudence de la CJUE et aux droits fondamentaux.)

Conservation des données ciblée visant des bâtiments stratégiques ou vulnérables

- Le projet de loi activerait la conservation des données de manière systématique et généralisée sur la zone d'infrastructures importantes car stratégiques, fort fréquentées, ou sensibles. La liste est longue et inclut les gares, autoroutes, parlements, hôpitaux …
  Tout le monde passe par les gares, aéroports, autoroutes… Cibler toutes ces infrastructures revient à surveiller de manière indifférenciée et généralisé une partie énorme de la population. Rappel : au Danemark ces zones sont très fort limitées : les résidences royales, les propriétés de la police et quelques infrastructures critiques telles que des « aéroports, les gares et les zones de péage. » Pour ce qui est de zones sensibles (comme les hôpitaux), il faudrait voir si la conservation des données est une mesure nécessaire à leur protection. L'exposé des motifs stipule que « [h]acker des hôpitaux par exemple constituerait une menace grave pour [les besoins essentiels de la population],» mais **d'autres mesures de protection** (logs, cybersécurité, protocoles, tests de pénétration, etc.) **peuvent et doivent être envisagées avant de recourir à la surveillance** par la conservation des données dans ces zones.

- Sur cette question du 'ciblage' peu ciblé, j'ai demandé à un ancien juge de a CJUE ce qu'il pensait. Dans son opinion juridique, Prof. Dr. iur. Vadapalas déclare (p31): Seuls les sites qui "reçoivent régulièrement un très grand nombre de visiteurs" et qui sont "particulièrement vulnérables à la commission d'infractions pénales graves" peuvent être couverts. Lister dans la loi tous les sites où transitent en Belgique beaucoup d'individus (tel que l'entièreté du réseau autoroutier), ne constitue pas un tel ciblage. (Il est tout aussi circonspect concernant la conservation des données dans le périmètre autour des zones ciblées.) Il ajoute (p32) en faisant référence au dernier arrêt de la CJUE (Garda Síochána §81) que **le ciblage géographique exécuté en simultané dans plusieurs zones est à exclure, parce qu'il acquière là un caractère général et perd donc son caractère 'ciblé'** ; c'est là l'interprétation d'un ancien juge de la CJUE, qui contraste complètement avec l'interprétation que le gouvernement belge a fait de cette même jurisprudence.
- À suivre l'opinion juridique de l'ancien juge de la CJUE Vadapalas (p34), il est clair que concernant les zones stratégiques ou vulnérables, le projet de loi tel que présenté "autoriserait des mesures de ciblage géographique » dans tellement de zones et de telle façon que cela transformerait la conservation 'ciblée' en une « conservation de données générale et indiscriminée sans établir les garanties juridiques nécessaires.»

Conservation des données ciblée visant des bâtiments des Institutions Internationales

Note : L'exposé des motifs explique que « *la Belgique est le siège d'un certain nombre d'institutions internationales qui, en raison de leur nature, peuvent faire l'objet de menaces graves. Il s'agit en premier lieu des bâtiments affectés à l'Union européenne, des bâtiments et infrastructures affectés à l'OTAN, des bâtiments des institutions de l'Espace économique européen et des bâtiments des Nations Unies. Selon ce critère, les bâtiments des ambassades et des représentations diplomatiques situés en Belgique sont également considérés comme des zones nécessitant la conservation de données*. »

- Si la rétention de données constitue une grave menace pour la démocratie au niveau national, je pense également que **le processus démocratique européen est menacé si les autorités et les services de renseignement belges sont en mesure d'accéder aux données de localisation, de trafic et de communication (métadonnées) des députés européens et de tous les individus qui mettent les pieds dans le périmètre entourant le Parlement.** En tant que membre du Parlement européen, mes conversations avec mes contacts confidentiels avec des citoyens, des journalistes et des informateurs seront enregistrés (et eux mêmes seront dans ce cas quand ils me rendront visite sur place), ce qui s'apparente à une ingérence grave et non proportionnée dans les droits fondamentaux des citoyens.
- **Cela vaut aussi pour les autres institutions. Une concertation au cas-par-cas devrait en tout cas être envisagée avant de mettre en place une telle mesure pour la protection de chaque institution internationale**, ce qui n'a pas été fait.
- De plus, **ces institutions ont déjà leurs propres protocoles et mesures de sécurité**, bien suffisants à priori pour répondre aux objectifs derrière ce projet de loi. Quand il n'y a aucune indication que ces zones aient été la cible de menaces ou crimes pertinents, les mesures de sécurité déjà présentes sur place devraient suffire, et aucune conservation des données préventive ne devrait être d'application.

Sur la question de couvrir ou non les OTT (services over the top)

- Même la Directive sur la conservation de données qui avait été annulée par la CJUE n'allait pas aussi loin !

- Une loi de surveillance couvrant les OTT capturerait tout contact confidentiel dans le privé, le professionnel et le gouvernement.

Sur la question de l'encryptage

- Il est crucial que ceux qui en ont besoin – que ce soit les avocats, les juges, les politiques, les gouvernements, les victimes d'abus ou les citoyens *lambda* – puissent avoir recours à l'encryptage. C'est une mesure de sécurité importante, comme reconnu par le gouvernement dans l'exposé des motifs (p17).
  Cependant, si la loi est suivie strictement jusqu'au bout, techniquement Signal devra se retirer du marché car il ne peut pas fournir les metadata sans mettre en peril l'encryptage de bout en bout (E2EE), qui est son argument de vente numéro un.
  Je ne sais pas quel appli est utilisée pour converser de manière 100 % sécurisée au sein du gouvernement belge, mais sachez que pour ce qui est des messages sur téléphone, la Commission Européenne demande de son personnel qu'il communique via Signal. En de facto interdisant à Signal d'offrir ses services en Belgique, le gouvernement belge est-il prêt à contraindre les Institutions internationales hébergées sur son sol à ne correspondre que par des services alternatifs, moins fiables et plus surveillables ?

- Il ne ressort pas clairement du projet de loi que les services permettant de surfer le web de façon anonyme et protégée, tels que TOR, seront couverts ou non. Dans le même esprit que Signal, ce genre de service est une nécessité, à l'ère où de plus en plus des aspects de nos vies sont digitalisés, scannés, fichés.
  Le Ministre van Quickenborne déclarait pendant la première réunion de la commission « Je ne suis pas en faveur d'un backdoor – on ne peut pas être en faveur d'un backdoor au sein d'une démocratie ». J'applaudis cette déclaration.

- Comme le montrent les derniers scandales liés à l'utilisation par des gouvernements européens du software Pegasus envers leur propres citoyens, **les gouvernement dits démocratiques ne sont pas exempts d'abus** – c'est pourquoi une nouvelle commission a été créée à ce sujet au Parlement Européen. La cybersécurité et la confiance envers l'État n'est pas donnée quand on est un activiste, journaliste d'investigation (ou sa source) ou opposant politique (voire avocat, conseiller, victime ayant besoin de l'anonymat), et **cette conservation des données (avec son impact sur l'encryptage) est un pas de plus affaiblissant cette cybersécurité et cette confiance.**

- Le gouvernement « estime approprié et proportionné d'imposer cette obligation » en partie parce qu'il considère que les données de trafic et de localisation « sont effectivement sensibles mais moins sensibles que leur contenu » (p20). Ce n'est pas l'avis de la CJUE qui, dans Garda Síochána, rappelle que les données relatives au trafic et les données de localisation « fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications » (§45)

Les adresses IP et autres données

- Le nouvel article 126 proposé prévoit la conservation extensive et systématique des données IP attribuées à la source de la connexion, ce qui permettrait l'identification, le suivi, le profilage et la localisation des utilisateurs. Il faut considérer que **la conservation des données IP, notamment avec la récente norme IPv6, permettrait maintenant d'établir**

des profils beaucoup plus détaillés des citoyens que ne le permettent les données de connexion téléphonique. La norme IPv6 permet d'attribuer une adresse IP unique à presque tous les appareils présents dans notre vie, ce qui a une incidence sur l'utilisation quotidienne de milliards d'appareils connectés/intelligents tels que les montres, les caméras, les portes, les jouets et les voitures, ainsi que les smartphones. De nombreux appareils collectent des données même en mode veille.

- La conservation indiscriminée des adresses IP et des données d'identification de tous les utilisateurs de services de communication dans l'UE, porte atteinte au droit d'utiliser Internet et de communiquer de façon anonyme. Cette mesure rendrait identifiables les contacts sociaux (y compris professionnels), les déplacements et la vie privée (par exemple les contacts avec les médecins, les avocats, les comités d'entreprise, les psychologues, les services d'assistance téléphonique, etc.) de millions d'Européens qui ne sont pas soupçonnés d'avoir commis un quelconque méfait. Cela permettrait de créer des profils complets de la personnalité et des mouvements de pratiquement chaque citoyen. Une fois qu'un pseudonyme ou un identifiant est identifié via l'adresse IP de l'utilisateur, les enregistrements d'activité permettent généralement de retracer le comportement en ligne. Combiné aux informations stockées par Google, Twitter ou Facebook, chaque recherche, clic, téléchargement et message devient potentiellement traçable. Comme la plupart des courriers électroniques comporte l'adresse IP de l'expéditeur, les courriers électroniques anonymes ou pseudonymes deviendront identifiables à l'avenir. L'adresse IP peut également être utilisée pour déterminer la localisation approximative de l'utilisateur, notamment s'il est chez lui, au travail ou en déplacement. Contrairement à ce qui est permis dans le projet de loi, l'arrêté portera donc sur « des métadonnées de communications électroniques qui donnent des informations … sur la localisation de l'équipement terminal,» entre autres.

- La conservation des adresses IP à la source peut donc être, selon la forme qu'elle prend, une forme de surveillance généralisée et indifférenciée des citoyens. La CJUE note la licéité d'une « conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, **pour une période temporellement limitée au strict nécessaire** ».[9] **Cet élément temporel manque à l'appel dans le projet de loi belge, ce qui le rend susceptible d'être abrogé ultérieurement. De plus, les nouvelles caractéristiques de l'IPv6 n'avaient pas encore été prises en compte par la Cour quand elle permettait cette conservation des adresses IP, ce qui (à la lumière de l'ingérence accrue) devrait conduire le législateur à la prudence et la nuance quand il la prévoit.**

- Le gouvernement propose de conserver non pas seulement les adresses IP, mais aussi de vastes autres catégories de données servant à identifier les utilisateurs finaux, tels que les données IMEI, IMSI et autres. Tout d'abord, comme le souligne l'APD (pp43-44) et *contra* l'exposé des motifs (pp42-45) les adresses IP suffisent dans bien des cas. Ensuite, le fait que la CJUE n'ait pas encore eu à se prononcer sur la proportionnalité d'une conservation de données autres que les adresses IP ne permet pas logiquement de dire, avec autant de facilité que le fait le gouvernement, que cette conservation n'est pas interdite. Un vrai examen de la proportionnalité ainsi que de ce qui est possible techniquement avec les IP est nécessaire, et manque à l'exposé des motifs (et le fait que les opérateurs aient demandé de pouvoir conserver ces autres catégories de données n'est pas en soi suffisant).

9 Garda Síochána, §67, emphase ajoutée.

Annexe : Article 90ter du Code d'instruction criminelle

(Note : mon emphase en **gras**, et ajouts explicatifs en **gras** après la référence aux articles)

§ 1. Le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, 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.
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.**
…
La mesure visée au présent paragraphe ne peut être ordonnée que pour rechercher les données qui peuvent servir à la manifestation de la vérité. **Elle ne peut être ordonnée qu'à l'égard soit de personnes soupçonnées, sur la base d'indices précis**, d'avoir commis l'infraction, **soit à l'égard des moyens de communication ou systèmes informatiques régulièrement utilisés par un suspect, soit à l'égard des lieux présumés fréquentés par celui-ci. Elle peut également être ordonnée à l'égard de personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.**

§ 2. Les infractions pouvant justifier la mesure visée au paragraphe 1er sont celles qui sont visées:
1° aux articles 101 à 110 du Code pénal; **attentat au roi/heritier/ministre**
2° aux articles 136bis, 136ter, 136quater, 136sexies et 136septies du même Code et à l'article 41 de la loi du 29 mars 2004 concernant la coopération avec la Cour pénale internationale et les tribunaux pénaux internationaux; **genocide, crime de guerre, ou aide à la préparation de tels crimes**
3° au livre II, titre Iter, du même Code; **empêcher quelqu'un d'exercer ou d'assister à son culte, par des troubles, des désordres, des menaces, des violences...**
4° à l'article 147 du même Code; **illégalement et arbitrairement arrêter ou faire arrêter, détenir ou fair détenir une ou plusieurs personnes**
5° aux articles 160, 161, 162, 163, 168, 171, 173 et 176 du même Code; **contrefaçon/altération de monnaies, obligations, billets**
6° aux articles 180 et 186 du même Code; **contrefaçon de timbres ou de moyens servant à la fabrication de timbres, billets, coupons etc.**
7° à l'article 210bis du même Code; **commettre un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données**
8° aux articles 246, 247, 248, 249 et 250 du même Code; **passive/active corruption (y compris spécifiquement quand cela concerne une personne qui exerce une fonction publique dans un Etat étranger ou dans une organisation de droit international public)**
9° à l'article 259bis du même Code; **intercepter ou fait intercepter, prendre connaissance ou faire prendre connaissance, enregistrer ou faire enregistrer des communications non accessibles au public, hors du cadre légal, et/ou les divulguer/utiliser**
10° à l'article 314bis du même Code; (same as above?)
11° aux articles 324bis et 324ter du même Code; **Constituer/participer dans une organisation criminelle préparant/commettant des crimes et délits punissables d'un emprisonnement de**

trois ans ou d'une peine plus grave, pour obtenir, directement ou indirectement, des avantages patrimoniaux

12° aux articles 327, 328, 329 et 330 du même Code, pour autant qu'une plainte ait été déposée; **menacer d'un attentat, sciemment donner une fausse information concernant l'existence d'un danger d'attentat**

13° à l'article 331bis du même Code; **menacer d'utiliser des matières ou engins radioactifs ou menace de commettre un acte dirigé contre une installation nucléaire ou de perturber le fonctionnement d'une telle installation, menacer de commettre un vol de matières nucléaires afin de contraindre une personne physique ou morale, une organisation internationale ou un Etat à faire ou à s'abstenir de faire un acte**

14° à l'article 347bis du même Code; **faire une prise d'otages**

15° aux articles 372 à 377bis du même Code; **attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de seize ans accomplis; viol**

16° à l'article 377quater du même Code; **proposer une rencontre à un mineur de moins de seize ans accomplis dans l'intention de commettre une infraction (ci-dessus)**

17° aux articles 379, 380 et 383bis, §§ 1er et 3, du même Code; **attenter aux moeurs en excitant, favorisant ou facilitant, pour satisfaire les passions d'autrui, la débauche, la corruption ou la prostitution d'un mineur de l'un ou de l'autre sexe; exploiter la débauche ou la prostitution d'une personne majeure (incl. tenir une maison de débauche ou de prostitution, louer des chambres dans ce but); exposer, offrir, vendre, louer, transmettre, fournir, distribuer, diffuser, ou mettre à disposition, du matériel pédopornographique ou le produire, importer ou faire importer**

18° à l'article 393 du même Code; **meurtre**

19° aux articles 394 et 397 du même Code; **assassinat**

20° aux articles 428 et 429 du même Code; **enlever ou faire enlever un mineur ou une personne vulnérable**

21° à l'article 433bis/1 du même Code; **communiquer avec un mineur en vue de commettre un crime/délit, en mentant sur son identité ou en insistant sur la discrétion**

22° aux articles 433quinquies à 433octies du même Code; **traite d'êtres humains**

[7 22/1°. aux articles 433novies/2 à 433novies/10 du même Code;]7 **vol ou prélèvement d'organe non-autorisé**

23° à l'article 434 du même Code; **ordonner hors du cadre légal l'arrestation ou la détention des particuliers**

24° aux articles 468, 470, 471 et 472 du même Code; **commettre un vol à l'aide de violences ou de menaces; extorqué, à l'aide de violences ou de menaces, soit des fonds, valeurs, objets mobiliers, obligations, billets, ... ou signature d'un document**

25° à l'article 475 du même Code; **meurtre commis pour faciliter le vol ou l'extorsion, soit pour en assurer l'impunité**

26° au livre II, titre IX, chapitre Ier, section 2bis, et chapitre Ierbis du même Code; **vols et extorsions en matières nucléaires**

27° aux articles 504bis et 504ter du même Code; **corruption privée**

28° à l'article 504quater du même Code; **se procurer un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique (l'utilisation normale) des données dans un système informatique**

29° à l'article 505, alinéa 1er, 1° du même Code lorsque les choses concernées ont été enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit visés à cet article; **receler, en tout ou en partie, les choses enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit**

30° à l'article 505, alinéa 1er, 2°, 3° et 4° du même Code; **dissimuler l'origine illicite de ces choses ou les utiliser en connaissance de cause**

31° aux articles 510, 511, alinéa 1er, et 516 du même Code; **mettre le feu à des édifices, ponts, chemins de fer, magasins, chantiers, véhicules, récoltes, forêts, etc.**

32° à l'article 520 du même Code, si les circonstances visées aux articles 510 ou 511, alinéa 1er, du même Code sont réunies; **même chose mais au moyen d'explosifs**

33° aux articles 550bis et 550ter du même Code; **accéder à un système informatique ou s'y maintenir, outrepasser son pouvoir d'accès à un système informatique, y compris pour modifier, accéder aux données ou commettre des dégâts [= aussi hacking]**

34° à l'article 2bis de la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes; **à titre onéreux ou gratuit, poser des actes préparatoires en vue de la fabrication, la vente, la livraison ou la fourniture illicite d'une substance visée au § 1er [drogues reprises dans la liste arrêtée par le Roi], ou en vue de la culture des plantes dont peuvent être extraites ces substances**

35° à la loi du 28 mai 1956 relative aux substances et mélanges explosibles ou susceptibles de déflagrer et aux engins qui en sont chargés;

36° article 1er de l'arrêté royal du 12 avril 1974 relatif à certaines opérations concernant les substances à action hormonale, antihormonale, anabolisante, bêta-adrénergique, anti-infectieuse, antiparasitaire et anti-inflammatoire, article précité visant des infractions punies conformément à la loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, désinfectantes ou antiseptiques."; **L'importation, l'exportation, la fabrication, le transport, la vente, l'offre en vente, la détention, la délivrance, l'acquisition à titre onéreux ou gratuit des substances à action hormonale, anti-hormonale, anabolisante, (bêta-adrénergique), anti-infectieuse, anti-parasitaire et antiinflammatoire, telles quelles ou en mélange [non-autorisées] par le Ministre de la Santé**

37° aux articles 77bis à 77quinquies de la loi du 15 décembre 1980 concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers; **trafic d'êtres humains**

38° à l'article 10, § 1er, 2°, de la loi du 15 juillet 1985 relative à l'utilisation de substances à effet hormonal, à effet antihormonal, à effet bêta-adrénergique ou à effet stimulateur de production chez les animaux; **celui dont on peut raisonnablement admettre qu'il sait ou devrait savoir qu'il commercialise des animaux auxquels des substances ont été administrées en infraction de la présente loi**

39° à l'article 10 de la loi du 5 août 1991 relative à l'importation, à l'exportation et au transit d'armes, de munitions et de matériel devant servir spécialement à un usage militaire et de la technologie y afférente; **négocier, exporter ou livrer à l'étranger ou posséder à cette fin, des armes, des munitions ou du matériel devant servir spécialement (à un usage militaire ou de maintien de l'ordre) ou de la technologie y afférente**

40° à l'article 145, §§ 3 et 3bis, de la loi du 13 juin 2005 relative aux communications électroniques; **réaliser frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite; utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages [= fraude]**

41° aux articles 8 à 11, 14, 16, 19, 1°, 2°, 3°, 5° et 6°, 20, 22, 27 et 33 de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, aussi appelée "Loi sur les armes"; **fabriquer, porter des armes etc.**

42° aux articles 21 à 26 de l'Accord de Coopération du 2 mars 2007 entre l'Etat fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à l'exécution de la

Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction, faite à Paris le 13 janvier 1993;

43° à l'article 47 du décret du parlement flamand du 15 juin 2012 concernant l'importation, l'exportation, le transit et le transfert de produits liés à la défense, d'autre matériel à usage militaire, de matériel de maintien de l'ordre, d'armes à feu civiles, de pièces et de munitions;

44° à l'article 20 du décret de la Région wallonne du 21 juin 2012 relatif à l'importation, à l'exportation, au transit et au transfert d'armes civiles et de produits liés à la défense;

45° à l'article 42 de l'ordonnance de la Région de Bruxelles-Capitale du 20 juin 2013 relative à l'importation, à l'exportation, au transit et au transfert de produits liés à la défense, d'autre matériel pouvant servir à un usage militaire, de matériel lié au maintien de l'ordre, d'armes à feu à usage civil, de leurs pièces, accessoires et munitions.]5

§ 3. La tentative de commettre un crime visé au paragraphe précédent peut également justifier une [5 mesure]5.

§ 4. Une infraction, visée aux articles 322 ou 323 du Code pénal, peut également justifier une [5 mesure]5, pour autant que l'association soit formée dans le but de commettre un attentat contre les personnes ou les propriétés visées au § 2 [ou de commettre le fait punissable visé à l'article 467, alinéa 1er, du Code pénal]. <L 2004-12-09/40, art. 14, 042; En vigueur : 03-01-2005>