14-06-2022

Objet: Lettre concernant le projet de loi sur la collecte et la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et la fourniture de ces données aux autorités

Mesdames et Messieurs les députés,

Vous discutez actuellement le projet de loi 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.

European Digital Rights (EDRi) est une association représentant 47 organisations qui défendent les droits et libertés dans l'environnement numérique à travers toute l'Europe. Notre réseau travaille sur la question de la rétention des données depuis près de vingt ans. Nos membres ont régulièrement dialogué avec les législateurs à propos des risques pour les droits fondamentaux qu'une telle mesure implique, ont fourni une expertise technique lorsque cela était possible et ont porté des lois devant les tribunaux en Irlande, en Autriche, en Allemagne, en République tchèque, au Royaume-Uni, en France, etc. lorsque celles-ci contrevenaient aux principes fondamentaux nationaux et européens. La Liga voor Mensenrechten, qui s'efforce d'élargir le soutien aux droits humains en Belgique, a contribué à ces efforts.

Nous saluons la tentative du législateur belge de mettre en place un cadre juridique conforme à la jurisprudence de la Cour de justice de l'Union européenne (CJUE) pour la rétention des données de trafic et de localisation. Les régimes de conservation des données qui sont illégaux en vertu du droit européen doivent être abandonnés et remplacés dès que possible par des solutions qui passent le test de stricte nécessité et proportionnalité établi par les tribunaux.

Il est donc essentiel que le nouveau projet de loi n'introduise pas de mesures qui reproduiraient les effets de la loi précédente sur les droits fondamentaux et qui seraient contraires aux arrêts de la Cour constitutionnelle belge et de la CJUE.

Malheureusement, à notre lecture, ce projet de loi, tel qu'il est et s'il est adopté sans ajustements adéquats, représenterait un danger pour les droits des personnes, tels que le droit à la vie privée et à la protection des données, la liberté d'expression et d'information, les libertés de la presse et les garanties du secret professionnel, et introduirait potentiellement un dangereux précédent pour les autres Etats membres de l'Union européenne.

Nous avons identifié les graves lacunes suivantes que le Parlement devrait corriger de toute urgence afin d'éviter une future invalidation par les cours:[1]

- **La stricte nécessité de la loi belge sur la conservation des données doit être prouvée et non présumée :** À l'époque de l'invalidation de la précédente loi sur la conservation des données par la

1 Pour des commentairesplus détaillés, nous vous recommandons de lire l'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, 05.2022, https://www.liguedh.be/wp-content/uploads/2022/05/Avis-LDH-DATA-RETENTION-2022-final.pdf

Cour constitutionnelle belge, les représentants de la police ont averti que sans conservation des données, la police deviendrait "sourde et aveugle" [2] et ont fait valoir qu'il s'agissait d'une mesure indispensable.[3] Toutefois, de simples déclarations politiques soulignant la valeur présumée de la conservation des données n'étayent pas suffisamment la nécessité de la conservation de masse des données de télécommunications dans le but d'enquêter sur des crimes. La simple utilité d'un instrument pour les autorités répressives ne satisfait pas au critère de légalité, y compris la nécessité et la proportionnalité. Il convient plutôt de procéder à une évaluation factuelle de l'efficacité de la mesure, ainsi que d'examiner les options moins intrusives qui pourraient permettre d'atteindre le même objectif.

- **La conservation ciblée des données ne doit pas conduire à une conservation massive de facto des données :** La jurisprudence de la CJUE n'autorise la conservation des métadonnées que pour une durée limitée, de manière ciblée déterminée par un critère géographique. La principale conclusion est que l'obligation de conserver les données de communications électroniques doit être l'exception et non la règle. Le projet de loi choisit certaines zones géographiques en fonction du taux de criminalité grave et de leur nature à être soumises à des risques élevés de crimes graves, comme les aéroports, les gares, etc. où les personnes présentes seraient placées sous rétention systématique de données. Le texte précise que " le gouvernement considère qu'il n'est pas impossible que l'ensemble du territoire national soit couvert par la rétention de données (...) Si cette hypothèse est rencontrée, il s'agira alors d'une rétention ciblée dans son approche mais généralisée dans ses conséquences ".[4] Cela irait à l'encontre de la définition même de "ciblé" : le seuil de criminalité doit donc être adapté. Enfin, la nouvelle législation couvrirait les fournisseurs de services over-the-top (OTT)[5] (tels que WhatsApp, Skype, Signal ou Facebook Messenger). Ces services ne peuvent pas mettre en œuvre un ciblage géographique de leurs utilisateurs et conserveront probablement des données sur l'ensemble du territoire belge. En outre, ils sont pour la plupart établis en dehors de la Belgique, et imposer ces exigences dans le droit national belge pourrait entrer en conflit avec le principe du pays d'origine du droit de l'UE.

- **La conservation ciblée des données devrait être fondée sur des critères objectifs et des données vérifiées** : Les données utilisées pour former les taux de criminalité par zone géographique proviendraient de la Banque nationale générale (BNG) dont on sait qu'elle contient de nombreuses erreurs, inexactitudes et mauvaises caractérisations. L'utilisation de la BNG comme référence statistique ne peut donc pas être utilisée pour justifier l'atteinte aux droits d'un si grand nombre de personnes.

- **La définition des infractions graves doit être restreinte :** La notion d'infractions graves telle que définie à l'article 90ter du code de procédure pénale et utilisée dans le projet de loi pour calculer

2 *The Brussels Times*, Phone data investigations: Belgian law could be hanging by a thread, 31.03.2021, https://www.brusselstimes.com/162697/phone-data-investigations-belgian-law-could-be-hanging-by-a-thread-piloce-constitutional-court-service-providers-record-european-court-justice-crime-privacy

3 *RTBF*, Lutte contre le terrorisme : la conservation des métadonnées doit être exceptionnelle, selon le Comité T, 18.03.2022, https://www.rtbf.be/article/lutte-contre-le-terrorisme-la-conservation-des-metadonnees-doit-etre-exceptionnelle-selon-le-comite-t-10958051

4 Page 12 du projet de loi, https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf

5 Les OTT sont des services de médias offerts directement aux téléspectateurs via l'internet. Les OTT contournent les plates-formes de télévision par câble, radiodiffusion et satellite, c'est-à-dire les types d'entreprises qui agissent traditionnellement en tant que contrôleurs ou distributeurs de ces contenus. Le terme a également été utilisé pour décrire les téléphones cellulaires sans opérateur, avec lesquels toutes les communications sont facturées comme des données, et qui remplacent les autres méthodes d'appel.

le taux de criminalité est trop large. Elle inclut des infractions de droit commun telles que la falsification informatique, la fraude informatique, le vol avec violence, la détention de stupéfiants et regroupe des infractions pouvant donner lieu à des seuils de peine différents de sorte que leur caractère grave ne semble pas objectivé. Par ailleurs, le projet de loi impose aux opérateurs de stocker systématiquement les données contenues dans le registre des détails des appels (CDR), les données de localisation des personnes suspectées d'une fraude ou d'une utilisation abusive d'un réseau de communications électroniques, ainsi que les données relatives au trafic nécessaires à la détection de cette fraude ou de cette utilisation abusive. Toutefois, la fraude ne constitue pas une infraction grave et cette obligation de conservation serait donc contraire au droit européen. En outre, les opérateurs de téléphonie mobile proposent de plus en plus souvent des plans de facturation forfaitaire à leurs abonnés, ce qui rend la conservation des CDR totalement inutile pour des raisons commerciales.

- **Seules les adresses IP sources peuvent être conservées en masse pour lutter contre les infractions graves :** La CJUE indique que seule la conservation générale et indifférenciée des adresses IP à la source d'une communication électronique devrait être accordée en tant qu'exception à l'interdiction générale de la conservation de données en masse. Le texte proposé permet la conservation massive de catégories de données au-delà de l'exception strictement définie par la Cour en incluant l'identifiant créé pour chaque appel, la date de début de l'abonnement ou de l'inscription au service, les données relatives au type de paiement ou le numéro d'identification du terminal de l'utilisateur final (International Mobile Equipment Identity, IMEI, Media Access Control, MAC ou Permanent Equipment Identifier, PEI). La liste devrait être limitée à ce que prescrit la CJUE et une limite à la durée de conservation des adresses IP devrait être fixée par le législateur en accord avec les exigences de la CJUE. Nous suggérons également la prudence en ce qui concerne la conservation des données IP car la nouvelle norme IPv6 permet de tirer des conclusions beaucoup plus détaillées sur la vie d'une personne que les données de connexion précédentes.[6] L'avocat général de la CJUE a confirmé que les problèmes découlant de l'utilisation du protocole IPv6 devraient être abordés dans un futur arrêt.[7]

- **La loi belge sur la conservation des données ne doit pas porter atteinte au cryptage** : Le projet de loi confirme qu'il "interdit un système de cryptage qui rend impossible la conservation par les opérateurs des données d'identification, de trafic ou de localisation".[8] Cette disposition va plus loin que l'obligation précédente de conservation des données, en vertu de laquelle un fournisseur n'était tenu de conserver que les données générées ou traitées par lui. Les données que le fournisseur ne collectait pas ne pouvaient pas être conservées. La nouvelle législation obligerait les fournisseurs à enregistrer ces données pour le compte du gouvernement, même si le fournisseur n'en voit pas la nécessité pour lui-même. Les conséquences pourraient être considérables, y compris à l'échelle mondiale, puisque les exigences obligeraient ces fournisseurs de services à modifier l'ensemble de leur système technique, mettant ainsi potentiellement en danger les utilisateurs se trouvant dans des États autoritaires. Cela signifie également que les services de communication tels que Signal deviendront illégaux en Belgique. Signal est un système de communication crypté sécurisé, sur lequel de nombreuses personnes (y compris des journalistes et des hommes politiques) comptent pour la sécurité et la confidentialité de leurs communications. Il ne collecte pas plus de données que nécessaire pour

6 L'IPv6 permet d'attribuer une adresse IP unique à presque tous les appareils de notre vie, notamment les appareils connectés tels que les montres, les portes, les jouets et les voitures.
7 CJUE, Opinion de l'Avocat Général, Cas joins C-793/19 and C-794/19, para. 83
8 Page 19 du projet de loi, https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf

fournir ses services. Le projet de loi mettrait donc en péril la disponibilité de Signal en Belgique et, partant, son utilisation par les citoyens et citoyennes belges.[9]

Je vous remercie de votre attention et reste à votre disposition pour toute question.

Je vous prie de recevoir, Madame, Monsieur, mes meilleures salutations.

Chloé Berthélémy
Conseillère politique
chloe.berthelemy@edri.org

9 Les récents projets des Pays-Bas visant à obliger les applications de chat, telles que WhatsApp, à créer des portes dérobées dans leur système pour accéder aux données ont été abandonnés après que la société a annoncé qu'elle cesserait de proposer ses services dans le pays. Voir Marc Hijink et Rik Wassens, 'WhatsApp dreigde uit Nederland te vertrekken om aftapplicht', *nrc*, 03.06.22, https://www.nrc.nl/nieuws/2022/06/03/whatsapp-dreigde-te-vertrekken-om-aftapplicht-a4132175