La réception en Belgique: Un nouveau cadre légal qui résout tout?

Réceptions comparées de la jurisprudence européenne sur la conservation et l'accès aux données en procédure pénale

Journée d'études Projet NTIS

Paris Nanterre

3 avril 2022

Prof. Dr Vanessa Franssen

Table des matières

Introduction

- Conservation des données de communications électroniques (ou « rétention des données » ou « data retention »)
  - Sujet technique, fort débattu
    - UE, Belgique: va-et-vient depuis plus de 10 ans!
    - Opposition « lutte contre la criminalité (grave) » et « protection de la vie privée/des données à caractère personnel »
  - Pertinence pratique majeure
    - Bien au-delà de la « cybercriminalité »
  - Caractéristiques et objectifs
    - Distinction avec les mesures d'enquête

Contexte européen (1)

- Charte
  - Art. 7 et 8 (et 11)
- Directive 95/46/CE -> RGPD
  - Principes et exceptions
- Directive « ePrivacy » (-> Règlement « ePrivacy »)
  - Principe de la confidentialité des communications électroniques (art. 5, § 1er):
    - Contenu et données relatives au trafic
    - Interdiction d'interception
  - Obligation d'effacer ou anonymiser les données de trafic (art. 6)

Contexte européen (2)

- Directive « ePrivacy » (-> Règlement « ePrivacy »)
  - Exceptions:
    - Consentement (art. 5, § 1er)
    - Objectifs commerciaux ou techniques (art. 5, § 2)
    - Conservation (art. 15):
      - Fins:
        - sauvegarder la **sécurité nationale** ou
        - assurer la prévention, la recherche, la détection et la poursuites **d'infractions pénales** ou d'utilisations non autorisées du système de communications électroniques
      - Durée limitée
      - Mesure nécessaire, appropriée et proportionnée

Contexte européen (3)

- Directive « data retention »
  - Basée sur l'art. 15 Directive « ePrivacy »
  - Données d'identification et de trafic/de localisation
  - Criminalité grave -> pas de définition, EM!
  - Conservation 6 mois à 2 ans à compter de la date de la communication

Contexte européen (4)

- La CJUE entre dans le jeu…
  - *Digital Rights Ireland*: Directive DR invalidée
  - Sort des législations nationales basées sur Directive DR?
    - Insécurité juridique!

Contexte européen (5)

- Premières réponses CJUE
  - *Tele2 Sverige e.a.*
    - Données de trafic et de localisation
    - Interdiction d'une conservation généralisée et indifférenciée, même pour lutter contre la criminalité grave, car ingérence grave
    - Conservation ciblée acceptable si criminalité grave
      - Critères objectifs, non discriminatoires
      - Limitée dans le temps (principe de proportionnalité)
      - Sur le territoire de l'UE
    - Accès: conditions matérielles et procédurales (+ notification)
  - *Ministerio fiscal*
    - « Données relatives à l'identité civile » = moins sensibles
    - Conservation (et accès) pas limitée à la lutte contre la criminalité grave

Les antécédents de la nouvelle loi belge

Conservation des données sous la loi du 29 mai 2016 (1)

- Loi du 29 mai 2016
  - Antécédents, contexte & objectifs
  - Régime de conservation des données
    - Législation à 2 niveaux
      - Loi du 13 juin 2005 relative aux communications électroniques: conservation
      - Code d'instruction criminelle (et d'autres lois): accès
    - Caractéristiques
      - Conservation généralisée, indifférenciée
      - Accès graduel: type de données, gravité de l'infraction

Conservation des données sous la loi du 29 mai 2016 (2)

- Données d'identification
  - Définition?
  - **Conservation**: **12 mois** à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé
  - **Accès**: art. 46*bis* C.i.cr.
    - Autorité compétente: PdR
    - Infractions < 1 an d'emprisonnement: production des données d'identification jusqu'à 6 mois précédant la décision du PdR
    - Infractions plus graves: 12 mois

Conservation des données sous la loi du 29 mai 2016 (3)

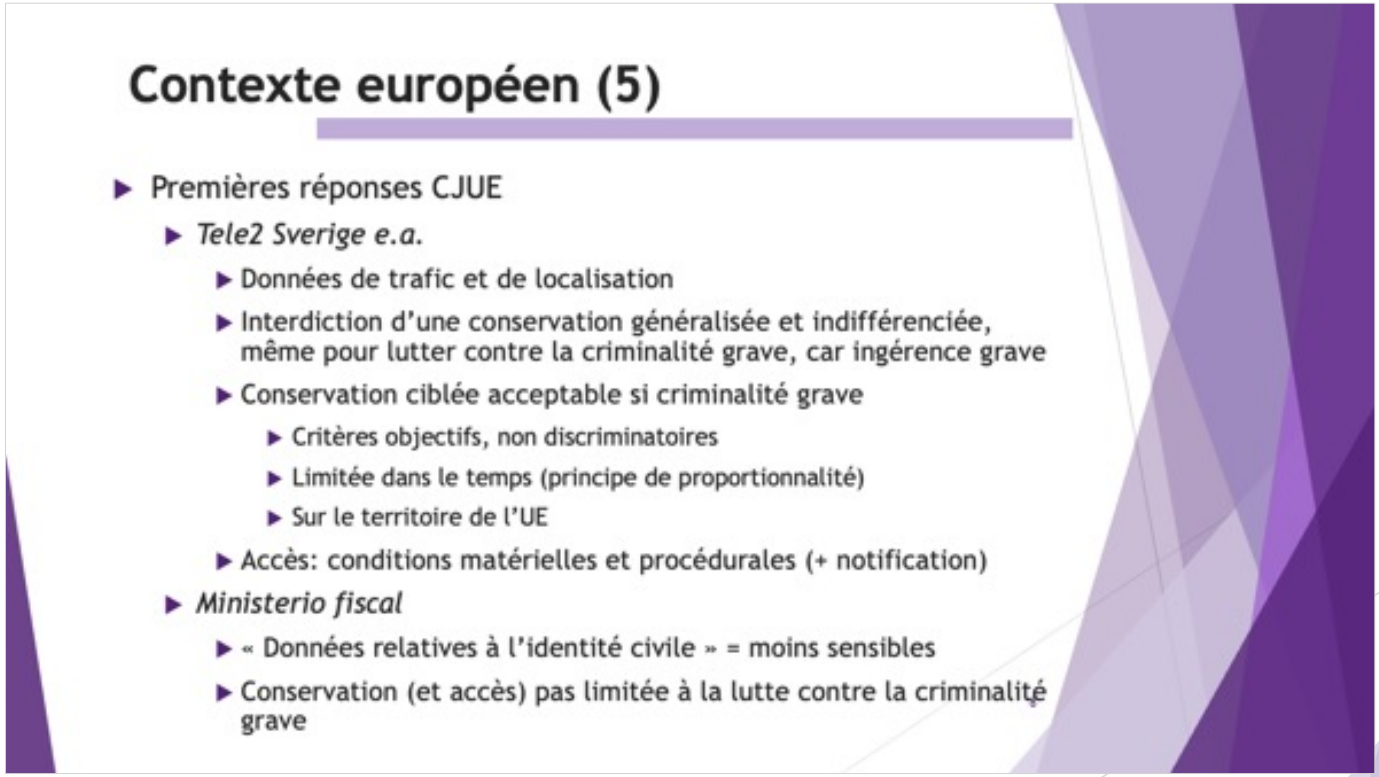
- Données de trafic et de localisation (ou « métadonnées », *infra*)
  - **Conservation**: **12 mois** à partir de la date de la communication
  - **Accès**: art. 88*bis* C.i.cr.
    - Autorités compétentes: JdI (mini-instruction) et parfois PdR
    - Infractions terroristes: jusqu'à 12 mois précédant le réquisitoire du JdI
    - Infractions visées à l'art. 90*ter*, §§ 2-4 C.i.cr./organisation criminelle/5 ans d'emprisonnement ou plus: 9 mois
    - Infractions moins graves, mais min. 1 an d'emprisonnement: 6 mois
    - Note: données futures aussi! ($\neq$ conservation des données)

Conservation des données sous la loi du 29 mai 2016 (4)

- Conformité avec le droit de l'UE?
  - Recours en annulation
  - Questions préjudicielles

L'arrêt *LQDN* et ses suites (1)

- *La Quadrature du Net e.a.*
  - Confirmation de *Tele2 Sverige* (*supra*, dia 8)



L'arrêt *LQDN* et ses suites (2)

- *La Quadrature du Net e.a.*
  - Mais certaines précisions et des « ouvertures »/« fissures »
    - Approche graduelle (fins, données)
    - Conservation généralisée et indifférenciée acceptable:
      - **données de trafic et de localisation** pour sauvegarder la **sécurité nationale** – mais conditions strictes!
      - **adresse IP de la source de la connexion** pour la lutte contre la **criminalité grave**
      - **données relatives à l'identité civile** pour la lutte contre la **criminalité**
    - Accès
      - Fin d'accès = fin de conservation (sauf si la fin d'accès est supérieure)

L'arrêt *LQDN* et ses suites (3)

- *La Quadrature du Net e.a.*
  - « Lapsus »?
    - Conservation rapide des données de trafic et de localisation
      - *Cf.* art. 16-17 Convention sur la cybercriminalité
      - *Cf.* art. 39*ter* C.i.cr. (voy. *infra*)
      - Conditions strictes!
        - Criminalité grave
        - Contrôle juridictionnel

L'arrêt *LQDN* et ses suites (3)

- *La Quadrature du Net e.a.*
  - « Lapsus »?
    - Conservation rapide des données de trafic et de localisation
      - *Cf.* art. 16-17 Convention sur la cybercriminalité
      - *Cf.* art. 39*ter* C.i.cr. (voy. *infra*, postface)
      - Conditions strictes!
        - Criminalité grave
        - Contrôle juridictionnel

L'arrêt *LQDN* et ses suites (4)

- Suite de *LQDN*
  - *Prokuratuur*, *Dwyer*, *Spacenet*
  - Confirmation et plus de précisions
    - Sécurité nationale >< criminalité grave
    - Critères objectifs et non discriminatoires
      - Zones géographiques
      - Personnes
    - Accès
      - Autorisation par une cour ou par une autorité indépendante
        - Autorité indépendante = ?

Incidences en droit interne (1)

- Réponse de la Cour constitutionnelle (arrêt n°57/2021 du 22 avril 2021)
  - Annulation de la loi du 29 mai 2016 – fidèle à *LQDN*
    - >< Conseil d'Etat français
  - Pas de maintien des effets juridiques
    - Car « niet » de la CJUE
  - Suggestion de recourir à l'art. 32 T.P.C.P.P.

Incidences en droit interne (2)

- Admissibilité des preuves
  - Art. 32 T.P.C.P.P.
    - Nullité de la preuve irrégulièrement obtenue si:
      - *« le respect des **conditions formelles concernées** est prescrit **à peine de nullité**, ou;*
      - *l'irrégularité commise a **entaché la fiabilité de la preuve**, ou;*
      - *l'usage de la preuve est contraire au droit à un **procès équitable**. »*

Incidences en droit interne (3)

- Admissibilité des preuves (suite)
  - Art 32 T.P.C.P.P. = conforme aux exigences de la CJUE?
    - A clarifier…
  - Distinction
    - Données déjà récoltées avant *LQDN*/(publication de l')arrêt de la C.const.
    - Données récoltées après/à l'avenir

Incidences en droit interne (4)

- Admissibilité des preuves (suite)
  - Distinction
    - Données déjà récoltées avant *LQDN*/(publication de l')arrêt de la C.const. -> art. 32 T.P.C.P.P. fonctionne « bien »
      - JP de la Cass.
        - Cass., 29 mars 2022, R.G. n°P.22.0078.N
        - Cass., 29 mars 2022, R.G. n°21.1422.N
        - Mais pas encore de jurisprudence de la Chambre francophone de la Cour de cassation!
      - Violation du droit au procès équitable?
        - Evaluation *in globo*
        - ≠ droit au respect de la vie privée/protection des données personnelles
        - Pas de violation parce que, entre autres:
          - Base légale en droit interne pour l'accès aux données conservées
          - Données pas déterminantes pour condamner (ont « juste » amenés les autorités à traquer les prévenus)
          - Contradiction possible

Incidences en droit interne (5)

- Admissibilité des preuves (suite)
  - Distinction
    - Données récoltées après/à l'avenir?
      - Plus d'obligation de conservation de données (sauf si données conservées de manière légale à d'autres fins (*supra*))
      - Illégalité connue des autorités belges
      - Art. 32 T.P.C.P.P. suffisant?

Incidences en droit interne (4)

- Nouvelle législation: loi du 20 juillet 2022
  - Enfin la bonne voie?

Analyse de la loi du 20 juillet 2022

Conservation des données - Aperçu des modifications de la loi du 13 juin 2005 relative aux communications électroniques

1. Nouvelles définitions : opérateurs et métadonnées
2. Conservation des données « générées ou traitées »
3. Conservation des données d'identification (art. 126)
4. Conservation des métadonnées (art. 126/1 & 126/2)
5. Critères de conservation (art. 126/3)
6. Accès aux données (art. 127/1)

Accès aux données dans le cadre judiciaire - Aperçu des modifications au Code d'instruction criminelle

1. Article 46*bis* - accès aux données d'identification
2. Article 88*bis* - accès aux métadonnées
3. Article 39*quinquies* – conservation rapide (« future freeze »)

Conservation des données
1. Nouvelle définition : opérateur

- Opérateur

« une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public »

(art. 2, 11° loi du 13 juin 2005)

→ Fournisseurs de réseaux (ex : Proximus, VOO, Telenet, Belnet, Universités, Administrations, etc.)

→ Fournisseurs de services (ex : Gmail, Hotmail, facebook, Messenger, Uber, WhatsApp, PlayStation, etc.) = services « OTT » « Over the Top »

Conservation des données
1. Nouvelle définition : métadonnées

- Métadonnées

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

(art. 2, 93° loi du 13 juin 2005)

Conservation des données
1. Nouvelle définition : métadonnées

- Métadonnées
  - = nouveau terme reprenant les « données de trafic et de localisation »
  - Données « autour » de la communication électronique
  - Exemples
    - Type de communication
    - Numéros appelés
    - Sites web visités
    - Lieu, date et heure de la communication
    - Durée d'un appel
    - Localisation
  - Pas le contenu

Conservation des données

2. Conservation des données « générées ou traitées » par les opérateurs

- Auparavant : liste de (méta)données à conserver « impérativement »
- Désormais : les opérateurs doivent conserver les (méta)données listées dans la loi « pour autant qu'ils les génèrent ou les traitent »
- Concrètement
  - Données générées : données créées par l'opérateur (ex. une adresse IP pour un fournisseur d'accès internet, un journal de connexion pour un service de messagerie électronique ou facebook, historique de commandes internet, etc.)
  - Données traitées : données utilisées par l'opérateur (ex. adresse IP de connexion au service, numéro de téléphone associé, compte bancaire associé, *device* associé, etc.)

Conservation des données

2. Conservation des données « générées ou traitées » par les opérateurs

Si opérateur ne génère ou ne traite pas les données listées dans la loi : pas d'obligation de les conserver

Exemple :

Application de messagerie Signal sur téléphone ne garde aucune trace de son utilisation et ne traite « que » le numéro de téléphone de l'utilisateur

→ seule cette donnée devra être conservée par l'opérateur de la messagerie Signal

Conservation des données

3. Conservation des données d'identification (art. 126)

- Peu de différences avec l'ancien système – conservation générale et indifférenciée pas remis en cause par la CJUE
- Nouveauté : énumération légale et non plus dans un arrêté royal
- 16 données à conserver par les opérateurs listées à l'article 126
- Possibilité pour le Roi de s'adapter aux évolutions technologiques + affiner la précision/la fiabilité des données à conserver
- But : identifier l'utilisateur d'un service ou les services utilisés par une personne

Conservation des données

3. Conservation des données d'identification (art. 126)

- 1° le numéro de Registre national ou un numéro équivalent, le nom et le prénom de l'utilisateur final qui est une personne physique ou la dénomination de l'abonné qui est une personne morale;
- 2° l'alias éventuel choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service;
- 3° les coordonnées de l'abonné qui ont été fournies lors de la souscription au service, notamment son numéro de téléphone, son adresse e-mail et son adresse postale;
- 4° la date et l'heure de la souscription au service et de l'activation du service et les éléments permettant de déterminer le lieu à partir duquel cette souscription et cette activation ont été effectuées, à savoir notamment:
- - l'adresse physique du point de vente où la souscription ou l'activation ont eu lieu, ou;
- - l'adresse physique du point de terminaison du réseau ayant servi à la souscription ou à l'activation, ou;
- - l'adresse IP ayant servi à la souscription ou à l'activation ainsi que le port source de la connexion et l'horodatage, ou;
- - dans le cadre d'un réseau téléphonique mobile, la localisation géographique de l'équipement terminal qui a permis la souscription ou l'activation au moyen d'un numéro de téléphone;
- 5° l'adresse physique de livraison du service;
- 6° l'adresse de facturation du service et les données relatives au type et au moyen de paiement, à la date des paiements, et la référence de l'opération de paiement en cas de paiement en ligne;
- 7° le service principal et les services annexes que l'abonné peut utiliser;
- 8° la date à partir de laquelle ces services peuvent être utilisés, la date de la première utilisation de ces services et la date de fin de ces services;
- 9° en cas de transfert de l'identifiant de l'abonné, tel son numéro de téléphone, l'identité de l'opérateur qui transfère l'identifiant et l'identité de l'opérateur auquel l'identifiant est transféré et la date à laquelle le transfert est effectué;
- 10° le numéro de téléphone attribué;
- 11° l'adresse de messagerie principale et les adresses de messagerie employées comme alias;
- 12° l'identité internationale d'abonné mobile, "International Mobile Subscriber Identity", en abrégé "IMSI";
- 13° l'identifiant permanent d'abonnement, "Subscription Permanent Identifier", en abrégé "SUPI";
- 14° l'identifiant caché d'abonnement, "Subscription Concealed Identifier", en abrégé "SUCI";
- **15° l'adresse IP à la source de la connexion, l'horodatage de l'attribution ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, les ports qui lui ont été attribués;**
- 16° l'identifiant de l'équipement terminal de l'utilisateur final, ou lorsque l'opérateur ne le traite pas ou ne le génère pas, l'identifiant de l'équipement qui est le plus proche de cet équipement terminal, à savoir notamment:
- - l'identité internationale d'équipement mobile, "International Mobile Equipment Identity", en abrégé "IMEI";
- - l'identifiant permanent de l'équipement, "Permanent Equipment Identifier", en abrégé "PEI";
- - l'adresse du contrôleur d'accès au réseau, "Media Access Control address", en abrégé "MAC";

Conservation des données

3. Conservation des données d'identification (art. 126)

- **Conformité jurisprudence CJUE et Cour Const. ?**
  - Données relatives à l'identité civile : non problématique dans le cadre de la lutte contre la criminalité « ordinaire »
  - Adresse IP attribuées à la source d'une connexion (°15) :
    - CJUE estime que ces adresses IP peuvent être utilisées pour tracer une personne et que leur conservation constitue une ingérence grave
    - Conservation n'est donc admissible que dans le cadre de la lutte contre la criminalité grave
  - Législateur en a tenu compte au niveau de l'accès aux données conservées (art. 127/1, §3 *in fine*):

une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.

Conservation des données

3. Conservation des données d'identification (art. 126)

- **Durée de conservation**
  - Article 126, § 2 : 12 mois
  - Pour certaines données, le point de départ de ce délai est à l'expiration de la session

Conservation des données

3. Conservation des données d'identification (art. 126)

- **Possibilité de s'adapter aux évolutions technologiques**
  - *17° les autres identifiants relatifs à l'utilisateur final, à l'équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.*
  - → Déterminé par le Roi
  - → À confirmer dans les 6 mois par la loi
  - Durée : fixée par le Roi dans un AR mais ne peut excéder 12 mois

Conservation des données

4. Conservation des métadonnées (art. 126/1 et 126/2)

- Énumération légale
- 10 données à conserver listées à l'article 126/2
- Possibilité pour le Roi de s'adapter aux évolutions technologiques + affiner la précision/la fiabilité des données à conserver

Conservation des données
4. Conservation des métadonnées (art. 126/2)

- 1° la **description et les caractéristiques techniques** du service de communications électroniques utilisé lors de la communication;
- 2° les **données d'identification** visées à l'article 126, § 1er, 2°, 10° à 14°, et 16°, du destinataire de la communication;
- 3° pour les services de communications électroniques à l'exception des services d'accès à Internet, **l'adresse IP** utilisée par le destinataire de la communication, **l'horodatage** ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués;
- 4° en cas d'appel multiple, de déviation ou de renvoi, **l'identification de toutes les lignes** en ce compris celles vers lesquelles l'appel a été transféré;
- 5° **la date et l'heure exacte du début et de la fin** de la session du service de communications électroniques concerné, en ce compris la date et l'heure exacte du début et de la fin de l'appel;
- 6° les données permettant **d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile**, qui ont été utilisées pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les **dates et heures** précises de ces différentes **localisations**;
- 7° le **volume de données** envoyées vers le réseau et téléchargées pendant la durée de la session;
- 8° pour ce qui concerne les services de communications électroniques mobiles, la **date et l'heure de la connexion** de l'équipement terminal au réseau en raison du démarrage de cet équipement et **le moment de la déconnexion** de cet équipement terminal au réseau en raison de l'extinction de cet équipement;
- 9° pour ce qui concerne les services de communications électroniques mobiles, la **localisation** de l'équipement terminal et **la date et l'heure de cette localisation** chaque fois que l'opérateur cherche à connaître quels équipements terminaux sont connectés à son réseau;

Conservation des données
4. Conservation des métadonnées (art. 126/1 et 126/2)

- **Possibilité de s'adapter aux évolutions technologiques**
  - *10° les autres identifiants relatifs au destinataire de la communication électronique, à son équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui* ***sont déterminés par le Roi, après avis de l'Autorité de protection des données et de l'Institut, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté****.*

→ Déterminée par le Roi

→ Après avis de l'Autorité de protection des données

→ À confirmer dans les 6 mois par la loi

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- Enseignements de la JP de la CJUE (*supra)*
  - « conservation générale et indifférenciée des métadonnées = exception et non la règle »
  - Suggestions de critères par la CJUE

- Législateur en a repris trois :
  - Critères géographique délimités sur la base de statistiques démontrant un nombre élevés d'actes de criminalité grave
  - Critère basé sur l'analyse de la menace
  - Critère basé sur des zones stratégiques/lieux sensibles

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critère géographique**
  - Basé sur les statistiques de la Banque de données générales de la police (« BNG »)
  - Seuil de criminalité grave défini par le législateur :
    - 3 faits constitutifs d'infractions visées à l'article 90*ter*, §§2 à 4 C.i.cr.
    - par an pour 1.000 habitants
    - sur une moyenne des 3 dernières années
    - par arrondissement judiciaire (ou zone de police)
  - Si ces critères sont remplis :
    - les métadonnées de communications électroniques seront conservées au niveau de l'arrondissement judiciaire

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critère géographique (suite)**
  - Délais de conservation également calculés sur une base statistique :
    - 6 mois si le seuil de 3/4 infractions listées à 90*ter*/1000 habitants est atteint
    - 9 mois si le seuil de 5/6 infractions listées à 90*ter*/1000 habitants est atteint
    - 12 mois si le seuil de 7/+ infractions listées à 90*ter*/1000 habitants est atteint

  - Si les seuils ne sont pas atteints au niveau de l'arrondissement judiciaire, le même calcul est effectué au niveau des zones de police
    - Ex. le seuil de 3 faits/1000 habitants n'est pas atteint sur le territoire de l'arrondissement du Luxembourg mais bien sur le territoire des zones de police d'Arlon et Bastogne
      - Conservation des données uniquement sur le territoire de ces zones de police

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critère basé sur l'analyse de la menace**
  - Critère lié de prime abord à la sauvegarde de la sécurité nationale
  - Mais notion de « Menaces » selon OCAM et Loi organique sur services de renseignements et de sécurité comprend :
    - Terrorisme
    - Extrémisme
    - Organisations sectaires nuisibles
    - Organisations criminelles

→ Domaines également couverts par la notion de « criminalité grave »

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critère basé sur l'analyse de la menace (suite)**
  - Métadonnées conservées dans les zones géographiques déterminées par l'OCAM si le niveau de menace pour ces zones est minimum de 3 (sur 4)
  - Si l'ensemble du territoire atteint ce niveau
    - Conservation générale et indifférenciée des données
    - Confirmation dans le mois par un AR sinon la mesure prend fin et opérateurs suppriment les données conservées sur cette base

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critères basé sur les zones stratégiques/lieux sensibles**
  - Article 126/3, §3 : zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave :
    - Infrastructures de transport (ports, aéroports, gares, stations de métro)
    - Bâtiments des douanes et accises, prisons, IPPJ, institutions de défense sociale
    - Armuriers et stands de tir
    - Infrastructures critiques (réseau ASTRID, sites SEVESO)
    - D'autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critères basé sur les zones stratégiques/lieux sensibles (suite)**
  - Art. 126/3, §4 : zones exposées à une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population :
    - Ordre public : zones neutres
    - Potentiel scientifique et économique : à lister dans un arrêté royal
    - Transport : autoroutes et parking attenants
    - Souveraineté nationale : Domaines royaux, Parlements, hôtels de police, maisons communales, domaines militaires, etc.
    - Intégrité du territoire : toutes les communes frontalières
    - Intérêts économiques et financiers : hôpitaux, BNB
    - Le cas échéant : autres zones à fixer dans un arrêté royal

Conservation des données
5. Critères de conservation des métadonnées (art. 126/3)

- **Critères basé sur les zones stratégiques/lieux sensibles (suite)**
  - Art. 126/3, §5 : zones exposées à une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national :
    - Ambassades
    - Bâtiments et infrastructures affectés à l'UE, l'OTAN, l'EEE et l'ONU
    - Le cas échéant, autres zones à fixer dans un arrêté royal

Conservation des données
6. Accès aux données

- Article 127/1 à 127/3 loi du 13 juin 2005

- Principe : seules les autorités compétentes pour l'objectif affiché de conservation peuvent avoir accès à ces données

- Accès doit être prévu et conditions d'accès fixées dans une norme législative formelle
  - En matière judiciaire : le Code d'instruction criminelle (*infra*)

Conservation des données
6. Accès aux données

- Article 127/1, §4

Les données conservées en vertu des articles 126/1 et 126/3 le sont, notamment, pour les autorités et finalités suivantes :

- les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité
- les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique
- les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques
- **les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave**

- Criminalité grave au sens de 127/1
  - *les faits pour lesquels il existe des indices sérieux : « qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88bis, § 1er, alinéa 1er, du Code d'instruction criminelle »*
  - = minimum un an d'emprisonnement

Conservation des données
6. Accès aux données

- Dans la pratique : articles 127/1, 127/2 et 127/3 loi du 13 juin 2005
  - Création d'une cellule de coordination auprès de chaque opérateur
  - Les autorités adresse leurs demandes à cette cellule
  - La demande doit comporter (127/1, §6):

    1° **l'identité de l'autorité demanderesse**, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service;

    2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central;

    3° **la base juridique** sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité;

    4° le délai de réponse souhaité.

Accès aux données dans le cadre judiciaire - Aperçu des modifications au Code d'instruction criminelle (rappel)

1. Article 46*bis* C.i.cr. - accès aux données d'identification
2. Article 88*bis* C.i.cr.- accès aux métadonnées
3. Article 39*quinquies* C.i.cr. – conservation rapide (« future freeze »)

Accès aux données dans le cadre judiciaire
1. Article *46bis* – accès aux données d'identification

- Article n'a pas été substantiellement modifié : principes restent les mêmes
- Autorités judiciaires (PdR et JdI) peuvent obtenir sur cette base accès aux données d'identification listées à l'article 126 loi 13 juin 2005
- En théorie, opérateurs devraient fournir toute donnée d'identification qu'ils possèdent, même sur une autre base (par ex. commerciale ou de facturation) et sans limite de durée vu la formulation de l'article *46bis* C.i.cr.
- En pratique, les opérateurs se limitent au « minimum légal »
- Définition d'opérateur redondante dans l'article *46bis* C.i.cr.

Accès aux données dans le cadre judiciaire
1. Article *46bis* – accès aux données d'identification

- Délai
  - Infractions punissables d'une peine d'emprisonnement de moins d'un an :
    - 6 mois préalablement à la commission de l'infraction
  - Infractions punissables d'une peine d'emprisonnement de plus d'un an :
    - 12 mois préalablement à la commission de l'infraction

Si, évidemment, la donnée permettant l'identification est listée à l'article 126 loi 13 juin 2005

Accès aux données dans le cadre judiciaire
1. Article *46bis* – accès aux données d'identification

- **Nouveautés – à titre d'info**
  - Trois nouveaux acteurs doivent désormais fournir les données d'identification à côté des opérateurs :
    - Les banques et organismes bancaires relativement aux transactions et services effectués en ligne
    - Centres fermés et lieux d'hébergement au sens de la loi du 15/12/1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers
    - Des autres personnes morales qui sont l'abonné d'un opérateur ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques

  → En pratique, déjà possible mais simplification du processus

Accès aux données dans le cadre judiciaire
2. Article 88*bis* – accès aux données de trafic et de localisation

- Vise les « métadonnées »
  - Harmonisation terminologique eût été heureuse
- Par qui?
  - JdI (mais possible en mini-instruction)
  - Quelques exceptions: PdR
- Infractions punissables d'un an d'emprisonnement (// article 127/1 loi 13 juin 2005)
- Anciens délais d'obtention réintroduits par la nouvelle loi
  - 12 mois pour les infractions terroristes
  - 9 mois pour les infractions listées à 90*ter*, commises dans le cadre d'une organisation criminelle ou de nature à entraîner un emprisonnement correctionnel de 5 ans ou une peine plus lourde
  - 6 mois pour les autres infractions

Accès aux données dans le cadre judiciaire
2. Article 88*bis* – accès aux données de trafic et de localisation

- **Nouveauté – à titre d'info**
  - Introduction d'un §3 - Protection des secrets professionnels des avocats et des médecins
    - Mesure d'obtention des données uniquement après avoir averti le bâtonnier ou le représentant de l'ordre provincial des médecins
    - JdI les informera des éléments qu'il estime relever du secret professionnel
    - Ces éléments ne seront pas consignés au procès-verbal

Accès aux données dans le cadre judiciaire
3. Article 39*quinquies* – conservation rapide (« future freeze »)

- Introduit par la nouvelle loi car, selon le législateur, « indispensable » dans le « nouveau » système qui ne comprend plus de conservation généralisée et indifférenciée
- **Objectif :** conserver rapidement et/ou pour le futur des données visées à l'article 88*bis* dans l'optique où elle ne serait pas conservée sur une autre base
- Pertinent pour la cohérence du « nouveau » système, mais peu d'utilité pratique si conservation généralisée dans les faits

Accès aux données dans le cadre judiciaire

3. Article 39*quinquies* – conservation rapide (« future freeze »)

- **Conditions**
  - Les données visées à l'article 88*bis* C.i.cr.
  - Pour des infractions peine punissable de minimum 1 an ou plus lourde
  - **Décision écrite et motivée** avec mentions obligatoires mais possibilité de le faire oralement en cas d'urgence et confirmation écrite dans les plus brefs délais
  - Durée de la mesure (2 mois max mais possible renouvellement) et durée de conservation (6 mois max mais possibilité de prolongation)
  - Accès aux données : même procédure que 88*bis*, soit via mini-instruction

- Plus-value?? (voy. aussi *infra*, postface)
  - Articulation avec 39*ter* C.i.cr. ?
  - Article 88*bis* permet déjà d'obtenir des métadonnées pour le futur en une seule procédure

Conclusions (1)

- Première évaluation de la nouvelle loi
  - Conservation des données = exception? (*cf*. CJUE)
  - Critères géographiques = conservation ciblée, nécessaire et proportionnée ?
  - Criminalité grave?
  - Accès autorisé par une autorité indépendante?
- Sort fort incertain!
  - (non moins de) 5 recours en annulation devant la Cour constitutionnelle (affaires 7907, 7929, 7930, 7931 et 7932)

Conclusions (2)

- Opposition niveaux national-européen difficile à maintenir
  - Dialogue de sourds?
- Besoin d'une solution au niveau européen

Merci de votre attention!

Questions?

vanessa.franssen@uliege.be

Pour plus de détails, voy. B. FLUMIAN et V. FRANSSEN, " Le nouveau cadre légal en matière de conservation des données électroniques : 'Old wine in new bottles' pour les autorités judiciaires ?", in FRANSSEN, V. et MASSET, A. (dir.), *Le droit pénal et la procédure pénale en constante évolution*, coll. Commission Université-Palais, Vol. 217, Liège, Anthemis, 2022, p. 315-359.

LIÈGE université

Postface:
Conservation rapide des données en droit belge (1)

- **Conservation rapide des données**
  - Introduite par la loi du 25 déc. 2016
  - Transposition (tardive) de la Convention sur la cybercriminalité (Conseil de l'Europe, Budapest, 2001)
  - Art. 39*ter* (national) et 39*quater* (transnational) C.i.cr.
    - Et nouveau: art. 39*quinquies* C.i.cr. – portée? *infra*
  - Champ d'application
    - Données susceptibles de perte ou de modification
    - Données stockées, traitées ou transmises au moyen d'un système informatique (= vaste!) >< Convention de Budapest: uniquement des données qui sont déjà stockées!
  - Objectif
    - En vue d'une injonction de production, saisie ou autre mesure d'investigation ultérieure
    - Pas forcément un « gel » de données! (càd. données pas forcement rendues inaccessibles à l'utilisateur)
      - = logique car les données ne sont pas saisies, toujours en possession de la personne à qui l'ordre de conservation a été adressé

Postface:
Conservation rapide des données en droit belge (2)

- **Conservation rapide des données** (suite)
  - Pour quelles infractions?
    - Crime ou délit
  - Durée limitée (90 jours, mais renouvelable)
  - OPJ (national) – PdR (transnational, coopération judiciaire)
  - Ordre à qui?
    - « *à une ou plusieurs personnes physiques ou personnes morales de conserver les données qui sont en leur possession ou sous leur contrôle* »
    - Champ d'application plus large que les art. 46*bis*, 88*bis* et 90*ter* C.i.cr.!
  - Conformité avec jurisprudence de la CJUE?
    - CJUE, 6 octobre 2020, *La Quadrature du Net*
      - Uniquement pour lutter contre la criminalité grave >< loi belge
      - Autorisation préalable du juge >< loi belge

Postface:
Conservation rapide des données en droit belge (3)

- **Conservation rapide des données** – nouvel art. 39*quinquies* C.i.cr.
  - Introduite par la loi du 20 juillet 2022 (conservation des données), entrée en vigueur: 18 août 2022

« *[1 § 1er. Lors de la recherche de crimes et délits, le* ***procureur du Roi*** *peut, s'il existe des* ***indices sérieux*** *que les* ***infractions*** *peuvent donner lieu à un* ***emprisonnement correctionnel principal d'un an ou à une peine plus lourde****, ordonner, par une décision écrite et motivée, à un ou plusieurs acteurs visés à l'alinéa 2, de conserver les données visées à* ***l'article 88bis, § 1, alinéa 1er****,* ***générées ou traitées par eux dans le cadre de la fourniture des services*** *de communications concernés, qu'il juge* ***nécessaires****.*

L'ordre visé à l'alinéa 1er peut être ***donné, directement*** *ou par l'intermédiaire du service de police désigné par le Roi, à:*

- l'opérateur d'un réseau de communications électroniques; et

- toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La ***décision écrite et motivée mentionne****:*

- le nom du procureur du Roi qui ordonne la conservation;

- l'infraction qui fait l'objet de l'ordre;

- les circonstances de fait de la cause qui justifient la conservation;

- l'indication précise d'un ou de plusieurs des éléments suivants: la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;

- le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;

- la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;

- la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

*En cas d'urgence, la conservation peut être ordonnée verbalement. L'ordre doit être confirmé dans les plus brefs délais dans la forme prévue à l'alinéa 3.***»**

Postface:
Conservation rapide des données en droit belge (4)

- **Conservation rapide des données** - nouvel art. 39*quinquies* C.i.cr. (suite)

« *§ 2. Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que* ***l'intégrité, la qualité et la disponibilité des données soit garantie*** *et à ce que les données soient conservées de manière sécurisée.*

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le ***secret****. Toute violation du secret est punie conformément à l'article 458 du Code pénal.*

Toute personne qui ***refuse de coopérer****, ou qui fait disparaître, détruit ou modifie les données conservées, est* ***punie*** *[2 d'une amende de cent euros à trente mille euros]2.*

§ 4. ***L'accès*** *aux données conservées conformément à cet article n'est possible qu'en application de* ***l'article 88bis****.]1* »

Postface:
Conservation rapide des données en droit belge (5)

- **Conservation rapide des données** – nouvel art. 39*quinquies* C.i.cr. (suite)
  - Champ d'application
    - Métadonnées visées à l'art. 88*bis* C.i.cr.
  - PdR
  - Indices sérieux
  - Quelles infractions?
    - Infractions punies d'un an d'emprisonnement ou plus
  - Accès aux données: art. 88*bis* C.i.cr.
  - Différence avec art. 39*bis*??
    - Pouvoirs!
    - Champ d'application: données et infractions
    - Objectifs? Lien avec la conservation des données (*infra*)
  - Plus-value? A voir…