POLICE FÉDÉRALE

Direction générale de la police judiciaire (DGJ)
Direction des unités spéciales (DSU)
National Technical & Tactical Support Unit (NTSU)
Central Technical Interception Facility (CTIF)

Avenue de la Cavalerie 2
1040 Bruxelles
Tél. : +32 (0)2 642 77 11
Fax : +32 (0)2 642 77 10
E-mail : dsu.ntsu.ctif.perm@police.belgium.eu

Obligations de collaboration des opérateurs de réseau et fournisseurs de services de communications électroniques

Informations générales concernant le cadre légal, les obligations, les indemnités ainsi que le projet et la plateforme TANK pour l'échange de données entre les parties concernées

OBJET:	**Brochure d'information**
DESTINATAIRES :	**Opérateurs de réseau** **Fournisseurs de services de communications électroniques**
GESTIONNAIRE DU DOSSIER :	Luc Beirens Tél. +32 2 642 76 48

TYPE DE DOCUMENT :	**BROCHURE INFORMATIVE**	CLASSEMENT :	**-**
RÉFÉRENCE :	**DSU/NTSU/264/2017**	PAGES :	**22**
DATE DE PUBLICATION :	**17/05/2017**	ANNEXES :	**-**
DEGRÉ DE CONFIDENTIALITÉ :	**PUBLIC**	RÉF PC :	**-**

Politie

Obligations de collaboration des opérateurs de réseau et fournisseurs de services de communications électroniques

Informations générales concernant le cadre légal, les obligations, les indemnités ainsi que la plateforme de collaboration TANK pour l'échange de données entre les parties concernées

Table des matières

1 Introduction générale concernant l'obligation de collaboration 4

2 Cadre légal 5

2.1 Introduction 5

2.2 Dispositions de base : respect de la vie privée et le secret des communications 5

2.3 Code d'instruction criminelle (CIC) 6

2.4 AR obligation de collaboration en cas de demandes judiciaires 7

2.5 Loi sur les services de renseignement 8

2.6 AR obligation de collaboration en cas de demandes des services de renseignement 8

2.7 Loi relative aux communications électroniques (LCE) 9

2.8 Arrêté royal rétention de données 10

2.9 Arrêté royal relatif à l'identification des utilisateurs de cartes prépayées 10

2.10 Arrêté ministériel sur le buffering et le filtrage des communications électroniques – en développement 11

3 Obligations des opérateurs et fournisseurs de services en matière de collaboration avec les autorités judiciaires et les services de renseignement 12

3.1 Mise sur pied d'une cellule de coordination Justice (CCJ) 12

3.2 Prévoir un préposé à la protection des données à caractère personnel 12

3.3 Prévoir une procédure interne pour la collaboration avec les autorités 13

3.4 Tenue d'un journal concernant les demandes et les réponses 13

3.5 Fourniture des statistiques annuelles concernant les demandes 13

3.6 Conservation générale de données 13

3.7 Protection des données 13

3.8 Conservation de données à la demande de l'agent compétent 13

3.9 Destruction ou anonymisation des données après conservation obligatoire 14

3.10 Obligation de fourniture d'informations concernant les services et leur protection 14

3.11 Obligation de collaboration pour avoir accès aux communications 14

3.12 Fourniture de données d'identification et de données concernant les services fournis 14
3.13 Fourniture de données de trafic et de localisation 14
3.14 Obligation d'interception et de fourniture des données interceptées 15
3.15 Synchronisation et précision des heures communiquées 15
3.16 Obligation de secret 15
4 Dispositions pénales 16
4.1 Faire disparaître, détruire ou altérer des données dont la conservation a été demandée 16
4.2 Non-respect de l'obligation de conservation imposée par la loi 16
4.3 Refus de collaborer ou pas de collaboration dans le délai demandé 16
4.4 Violation de l'obligation de secret 16
5 Indemnités de collaboration 17
5.1 Principes généraux concernant l'indemnisation des opérateurs et fournisseurs de services 17
5.2 Les services indemnisés spécifiques avec un tarif propre 17
5.3 Demandes spécifiques 17
5.4 Autres services couverts par un forfait 18
5.5 Distinction entre grands et petits opérateurs 18
5.6 Les services indemnisés à partir d'un forfait annuel pour les grands opérateurs 18
5.7 L'indemnisation des petits opérateurs 19
6 Rôle du NTSU CTIF 19
7 Compétence de régulation des autorités en matière d'échange des données 19
8 Projet Tank 20
8.1 Description générale du projet 20
8.2 Architecture 20
8.3 Définition des formats de réponse standard 21
8.4 Calendrier du projet 21
8.5 Possibilités d'intégration avec TANK 21
8.6 Obligations de collaboration concernant TANK 21
9 Engagement en vue d'obtenir l'indemnité forfaitaire annuelle en tant que petit opérateur 23
9.1 Identification de l'opérateur 23
9.2 Inscription de la CCJ et coordonnées 23
9.3 Nomination d'un préposé à la protection des données à caractère personnel 23
9.4 Engagement de collaboration via la plateforme TANK 23
9.5 Demande d'indemnité en tant que petit opérateur 23

1 Introduction générale concernant l'obligation de collaboration

Dans la société actuelle, où pratiquement tout le monde utilise des moyens de communications électroniques et des systèmes informatiques, il est nécessaire que les différentes autorités puissent également effectuer des recherches dans cet environnement virtuel afin de faire respecter les droits de la société et des citoyens, ainsi que de pouvoir rechercher, identifier et localiser les suspects et, le cas échéant, obtenir des informations sur leurs communications ou intercepter celles-ci.

Ces recherches sont naturellement impossibles sans la collaboration des opérateurs de réseau ou des fournisseurs de services de communications électroniques (ci-après dénommés individuellement « opérateur » et « fournisseur de services »).

Dans ce cadre, le législateur a attribué diverses compétences à certains services de renseignement et autorités judiciaires, d'une part, et a imposé diverses obligations aux opérateurs et fournisseurs de services, d'autre part.

En exécution des dispositions légales, diverses autorités ont été impliquées afin de mettre sur pied cette collaboration entre les autorités et les opérateurs et fournisseurs de services. Les autorités veillent à ce que cette collaboration se déroule de la manière la plus efficace et économique possible. Ainsi, le service NTSU CTIF de la Police fédérale a désigné un certain nombre de formes de collaboration en tant qu'intermédiaire compétent pour l'échange de demandes et réponses entre les autorités, d'une part, et les opérateurs et fournisseurs de services, d'autre part.

Une plateforme d'échange, baptisée TANK, est en cours de développement afin d'automatiser l'échange de données. À l'avenir, la connexion à cette plateforme sera une condition sine qua non pour les opérateurs et les fournisseurs de service en vue d'une indemnisation par les autorités pour leur collaboration. À l'heure actuelle, le cadre légal exige que les opérateurs s'engagent à utiliser cette plateforme dès que celle-ci sera disponible.

L'objectif du présent document est de donner un bref aperçu du cadre légal, des compétences, des demandes de collaboration possibles, des obligations des opérateurs, des dispositions pénales, du rôle des différentes autorités, du projet TANK et de la demande d'engagement en tant qu'opérateur ou fournisseur de services.

Le présent document n'a pas pour vocation d'être exhaustif. Il s'agit d'une ébauche pour toute personne souhaitant acquérir des informations sur la collaboration entre les autorités, d'une part, et les opérateurs et fournisseurs de services, d'autre part.

Nous espérons que le présent document améliorera la collaboration entre les parties concernées.

Luc Beirens
Chef CTIF

2 Cadre légal

2.1 Introduction

Le cadre légal définissant la collaboration entre un opérateur d'un réseau ou le fournisseur de services de communications électroniques avec les autorités est constitué par une série d'articles répartis dans différents arrêtés royaux et lois.

Vous trouverez ci-dessous un aperçu des principaux articles de ces lois et arrêtés royaux (AR) avec une brève description du contenu et de l'autorité compétente pouvant demander cette collaboration. Une lecture approfondie de ces articles est nécessaire pour les opérateurs et fournisseurs de services afin de pouvoir estimer leur portée totale.

En outre, cet aperçu se limite à la collaboration avec les autorités judiciaires et les services de renseignement. D'autres autorités possèdent également des moyens pour interroger les opérateurs et fournisseurs de services, mais cela ne fait pas partie de la portée du présent document.

2.2 Dispositions de base : respect de la vie privée et secret des communications

La vie privée et familiale de toute personne est garantie par l'article 22 de la Constitution et par l'article 8 de la CEDH (Convention européenne des droits de l'homme). Toute dérogation à ce principe est uniquement possible sur la base d'une loi. Selon la jurisprudence nationale et internationale, les communications d'une personne sont couvertes par cette protection.

Le Code pénal belge définit aux articles 259bis et 314bis que l'interception de communications privées est punissable. Des articles définissent également que l'installation d'un appareil pour intercepter ces communications est punissable ainsi que l'utilisation ou la commercialisation d'informations obtenues via une interception illégale.

La loi relative aux communications électroniques (LCE) développe aux articles 122 à 127 la protection des communications électroniques et dispose qu'il est interdit de prendre connaissance de l'existence de communications électroniques, de l'identité et de la localisation des parties concernées ainsi que du contenu des communications. Il est interdit de conserver les données de ces communications à moins de les rendre anonymes ou sauf si une autre disposition légale le permet ou l'impose.

La LCE définit également les cas et les circonstances permettant de déroger légalement aux principes de base. Elle définit les données concernant les communications électroniques qui doivent être conservées et cite les autorités qui peuvent demander ces données. Plusieurs AR développent davantage l'obligation de conservation ainsi que les modalités pour l'identification des utilisateurs.

Le Code d'instruction Criminelle et la loi sur les services de renseignement et de sécurité prévoient les compétences et les conditions en vertu desquelles les autorités compétentes peuvent demander les données concernant les communications électroniques ou en vertu desquelles ces autorités peuvent intercepter légalement des communications électroniques ou requérir la collaboration d'un opérateur ou d'un fournisseur de services. Ces lois obligent les opérateurs ou fournisseurs de services à collaborer avec les autorités requérantes.

2.3 Code d'instruction Criminelle [1] (CIC)

Art	Description	Compétence
39ter	Conservation des données désignées	Officier de Police judiciaire
39quater §2	Conservation des données désignées à la demande d'autorités étrangères	Par le service de police désigné par le Roi
46bis	Demande de données concernant • L'identification des utilisateurs / appareils • Les services	Procureur du Roi directement ou via le service de police désigné par le Roi
88bis	Demande des données de trafic et de localisation tant historiques qu'en temps réel	Juge d'instruction Procureur dans certains cas directement ou via le service de police désigné par le Roi
90ter 90quater §2	Interception de communications	Juge d'instruction Procureur dans certains cas directement ou via le service de police désigné par le Roi
90ter 90quater §4	Fournir des renseignements / collaborer pour (pouvoir) accéder aux communications ou systèmes	Juge d'instruction Procureur dans certains cas directement ou via le service de police désigné par le Roi
464/13	Cf. art 46bis mais dans le cadre d'une enquête pénale d'exécution	Magistrats du tribunal de l'application des peines
464/25	Cf. art 88bis mais dans le cadre d'une enquête pénale d'exécution	Magistrats du tribunal de l'application des peines
464/26	Cf. art 90ter et suiv. mais dans le cadre d'une enquête pénale d'exécution	Magistrats du tribunal de l'application des peines

[1] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_name=loi
(pour les dispositions en matière d'information et d'instruction)
http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808121230&table_name=loi
(pour les dispositions en matière d'enquête pénale d'exécution)

2.4 AR obligation de collaboration en cas de demandes judiciaires

AR 9 JANVIER 2003. - Arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques[2]

Art	Description
1	Définitions
2	Obligation d'avoir une CCJ sur le territoire belge Possibilité de CCJ commune Avis de sécurité concernant les membres de la CCJ Disponibilité en permanence de la CCJ Communication de données (et de leur modification) concernant la CCJ et ses membres à l'IBPT Obligation de sécurisation des données de la CCJ et garantie de la confidentialité
3	Collaboration pour identifications art. 46bis – désignation NTSU CTIF Compétence NTSU CTIF en matière d'accès aux données des clients Compétence NTSU CTIF en matière de règlement de ce transfert de données
4	Collaboration pour les données de trafic et de localisation en temps réel ou historiques Délai de réponse Compétence de l'autorité pour le règlement du format et du mode de transfert
5	Collaboration pour l'interception de communications électroniques Désignation du NTSU CTIF en tant que service central auquel transmettre les communications interceptées
6	Obligation de pouvoir satisfaire aux demandes des autorités Exigences en termes de qualité des données transmises : transmission contrôlable, en clair Transmission en temps réel de manière sécurisée Normes ETSI et 3GPP à respecter – compétence des autorités dans le choix des options
8	Obligation de synchronisation des systèmes de l'opérateur Précision des heures communiquées
10	Dispositions concernant les frais d'investissement, d'exploitation et d'entretien Renvoi à l'annexe en ce qui concerne les indemnités
10bis	Compétence des autorités pour déterminer le format et le mode de transmission Obligation de communication des informations si la transmission par voie électronique n'est pas possible
Annexe N	Informations sur les indemnités dans le cadre de la collaboration Définitions : demande / critère de demande / demande spécifique Tarifs des prestations Forfait annuel Possibilité de réaction en cas d'accumulation de demandes

[2] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2003010942&table_name=loi

2.5 Loi sur les services de renseignement

Loi du 30 NOVEMBRE 1998. - Loi organique des services de renseignement et de sécurité [3]

Art	Description	Compétence
18/7	Demande de données concernant • L'identification des utilisateurs / appareils • Les services	Dirigeant du service de renseignement Officier de renseignement dans certains cas
18/8	Demande des données de trafic et de localisation tant historiques qu'en temps réel	Dirigeant du service de renseignement Officier de renseignement dans certains cas
18/17	Interception de communications Prêter assistance pour pouvoir avoir accès	Dirigeant du service de renseignement après l'accord de la Commission BIM

2.6 AR obligation de collaboration en cas de demandes des services de renseignement

AR 12 OCTOBRE 2010. - Arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité [4]

Art	Description
1	Définitions
2	Obligation d'avoir une CCJ sur le territoire belge Possibilité de CCJ commune Avis de sécurité concernant les membres de la CCJ Disponibilité en permanence de la CCJ Communication de données (et de leur modification) concernant la CCJ et ses membres à l'IBPT Obligation de sécurisation des données de la CCJ et garantie de la confidentialité
3	Collaborations pour les identifications art 18/7 Compétence des services de renseignement en matière d'accès aux données des clients Compétence des services de renseignement en matière de règlement de ce transfert de données
4	Collaboration pour les données de trafic et de localisation en temps réel ou historiques Délai de réponse Compétence de l'autorité pour le règlement du format et du mode de transfert
5	Collaboration pour l'interception de communications électroniques Désignation du point de connexion au réseau défini par le dirigeant du service de renseignement
6	Compétence des autorités pour déterminer le format et le monde de transmission Obligation de communication des informations si la transmission par voie électronique n'est pas possible
7	Dispositions concernant les frais d'investissement, d'exploitation et d'entretien Renvoi à l'annexe de l'AR obligation de collaboration en cas de demandes judiciaires pour les indemnités liées aux demandes des services de renseignement

[3] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1998113032&table_name=loi
[4] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2010101212&table_name=loi

8	Obligation de pouvoir satisfaire aux demandes des autorités Exigences en termes de qualité des données transmises : transmission contrôlable, en clair Transmission en temps réel de manière sécurisée Normes ETSI et 3GPP à respecter – compétence des autorités dans le choix des options Obligation de synchronisation des systèmes de l'opérateur Précision des heures communiquées

2.7 Loi relative aux communications électroniques [5] (LCE)

Loi du 13 JUIN 2005. - Loi relative aux communications électroniques

Art	Description
122	Principes de base de traitement des données de trafic (effacer/anonymiser) et exceptions pour : • Obligation légale • Facturation • Marketing • Détection des fraudes
123	Principes de base du traitement des données de localisation et exceptions
124	Principe général d'interdiction de prise de connaissance, d'identification, d'interception et d'utilisation de ces informations
125	Exceptions à l'art. 124 de la loi et aux art. 259bis et 314bis du Code pénal (interception) • Si la loi l'impose • Contrôle bon fonctionnement / exécution • Services de secours et d'urgence • IBPT, JI, PdR, Dirigeant de la VSSE, SGRS • Service de médiation pour les télécommunications • Agents du SPF Économie • Commission d'éthique pour les télécommunications • Empêcher les communications électroniques non souhaitées / stalking
126 §1er	Obligation de conservation générale des données de trafic
126 §2	Autorités qui peuvent demander ces données • Autorités judiciaires • Services de renseignement et de sécurité • Services d'urgence • Officiers IBPT • Officier de police judiciaire de la Cellule des personnes disparues • Service de médiation pour les télécommunications
126 §3	Définition du délai de conservation et renvoi à l'AR pour les données.
126 §4	Obligation de : • Garantir la qualité et protéger les données • Protéger les données contre la destruction, l'altération, la divulgation ou l'accès non autorisé • Traitement uniquement par les membres de la cellule de coordination • Conserver sur le territoire de l'UE • Mesures de protection technologique

[5] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi

	• Tenue d'un journal concernant l'utilisation des données conservées
126/1	Obligations que la cellule de coordination doit respecter • Création de la cellule de coordination • Possibilité de cellule de coordination commune • Avis de sécurité pour les membres de la cellule de coordination • Mise au point d'une procédure interne de traitement des demandes • Prévoir un préposé à la protection des données à caractère personnel
127 §1er	Compétence des autorités d'imposer des mesures administratives / techniques concernant l'identification de l'utilisateur
127 §2	Interdiction d'utiliser une technologie empêchant l'identification / la localisation / l'interception
127 §3	Obligations pour les services avec carte prépayée

2.8 Arrêté royal rétention de données[6]

19 SEPTEMBRE 2013. - Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques

Art	Contenu de l'article
2	Définitions
3	Concernant la téléphonie fixe : données d'identification / données de trafic et de localisation
4	Concernant la téléphonie mobile : données d'identification / données de trafic et de localisation
5	Concernant l'accès à l'internet : données d'identification / données de trafic et de localisation
6	Concernant les services de courrier électronique : données d'identification / données de trafic et de localisation
7	Obligations en cas de combinaison des services offerts Précision de l'heure / synchronisation
8	Obligations concernant le préposé à la protection des données à caractère personnel
9	Obligation de fourniture de données statistiques à l'IBPT

2.9 Arrêté royal relatif à l'identification des utilisateurs de cartes prépayées [7]

Arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.

Art	Contenu de l'article
1	Champ d'application : Numéro de téléphone BE / IMSI BE Exclusion de l'identification : Cartes M2M
2	Définitions : document d'identification / méthode d'identification
3 – 6	Obligations de l'utilisateur final en matière d'identification et de notification de vol/perte
7	Principe de base de l'identification obligatoire

[6] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2013091920&table_name=loi
[7] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2016112703&table_name=loi

8	Obligation de désactivation en cas de notification de perte / vol
9	Obligation de vérification selon les méthodes d'identification valides
10	Autorisation de lecture / scan / photographie de la carte d'identité
11	Vérification obligatoire que la carte d'identité BE n'a pas été volée ou n'a pas fait l'objet d'une fraude Actions à entreprendre en cas de constatation d'irrégularités
12	Données pouvant être conservées pour identification
13	Obligation de proposer au moins une méthode d'identification valide
14	Conditions d'identification physique de l'utilisateur
15	Conditions d'identification via la carte d'identité électronique
16	Conditions d'identification via un fournisseur de service d'identification agréé
17	Conditions d'identification par transaction de paiement en ligne
18	Conditions en cas d'extension du produit
19	Conditions d'identification via un moyen de communications électroniques

2.10 Arrêté ministériel sur le buffering et le filtrage des communications électroniques – en développement

(Projet d') Arrêté ministériel portant exécution de l'article 6, § 3, deuxième alinéa, et de l'article 10bis, deuxième alinéa de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques

Cet AM définira les conditions concernant :

- La capacité de mise en mémoire tampon que les opérateurs doivent prévoir en cas de perte de la connexion entre l'opérateur et le NTSU CTIF.

- Les possibilités de filtrage qu'un opérateur doit pouvoir appliquer sur un flux de données intercepté avant de les transmettre au NTSU CTIF. L'objectif de ce filtrage est de limiter l'interception des communications électroniques au strict minimum sur la base de la décision du juge d'instruction.

Le projet d'AM a déjà fait l'objet d'une discussion avec le secteur mais doit encore être publié.

3 Obligations des opérateurs et fournisseurs de services en matière de collaboration avec les autorités judiciaires et les services de renseignement

Nous résumons succinctement les principales obligations des opérateurs et fournisseurs de services issues de l'aperçu des différentes dispositions légales.

3.1 Mise sur pied d'une cellule de coordination Justice (CCJ) [8]

Afin de protéger au maximum la confidentialité des recherches des autorités compétentes et la vie privée des personnes visées, le législateur a choisi de limiter le plus possible le groupe de personnes effectuant ces tâches au sein de chaque opérateur et fournisseur de services.

Il est obligatoire de mettre sur pied une cellule de coordination, dont les coordonnées doivent être communiquées à l'IBPT.

Le personnel de cette cellule doit faire l'objet d'un examen conformément à la procédure décrite à l'article 126/1 LCE. L'avis de sécurité doit être renouvelé tous les 5 ans.

La loi permet à plusieurs opérateurs et/ou fournisseurs de services de travailler avec une CCJ commune.

La CCJ doit être établie sur le territoire belge.

Seuls les membres de la CCJ peuvent prendre connaissance des demandes et y répondre.
Les membres de la CCJ peuvent se faire assister par des techniciens si cela est strictement nécessaire pour l'exécution du service requis.

3.2 Prévoir un préposé à la protection des données à caractère personnel [9]

Vu l'importance accordée par notre société à la protection de la vie privée, chaque opérateur et fournisseur de services est tenu de désigner un préposé à la protection des données à caractère personnel.

Ce préposé doit veiller :

- à ce que la société et la CCJ respectent les dispositions légales
- à ce que seules les données prévues par la loi soient conservées
- à ce que seules les autorités compétentes aient accès aux données conservées
- aux mesures de sécurité et de protection

La loi permet à plusieurs opérateurs et/ou fournisseurs de services de travailler avec un préposé commun à la protection des données à caractère personnel.

Les coordonnées de ce préposé doivent être communiquées à la Commission de la protection de la vie privée.

[8] Art 126/1 §1 LCE, art 2 AR obligation de collaboration Justice, art 2 obligation de collaboration services de renseignement
[9] Art 126/1 §3 LCE

3.3 Prévoir une procédure interne pour la collaboration avec les autorités [10]

Chaque opérateur et fournisseur de services doit établir une procédure interne pour ses collaborateurs de la CCJ et pour les techniciens d'assistance expliquant dans quel cadre légal cette aide est octroyée et quelles sont les obligations et conditions devant être respectées.

3.4 Tenue d'un journal concernant les demandes et les réponses [11]

Chaque opérateur et fournisseur de services doit tenir à jour un journal contenant les demandes et les réponses fournies. En particulier, ce journal doit mentionner l'ancienneté des données demandées et dans quels cas aucune réponse n'a pu être fournie à l'autorité requérante.

Ce journal doit pouvoir être consulté par la Commission de la protection de la vie privée. Cette dernière peut également en exiger une copie.

3.5 Fourniture des statistiques annuelles concernant les demandes [12]

Afin de permettre à l'autorité d'adapter sa politique et de distribuer les indemnités de manière légitime, les opérateurs et les fournisseurs de services doivent communiquer chaque année les chiffres concernant leur collaboration à l'IBPT.

3.6 Conservation générale de données

L'article 126 LCE, l'AR Rétention de données et l'AR Données d'identification des cartes prépayées définissent quelles données relatives aux communications électroniques doivent être conservées afin de pouvoir satisfaire aux demandes d'identification d'utilisateurs ou de moyens de communication ainsi que de fourniture de données de trafic et de localisation.

Les données doivent être conservées sur le territoire de l'Union européenne.

3.7 Protection des données

L'opérateur ou le fournisseur de services doit prendre toutes les mesures organisationnelles et techniques nécessaires afin de protéger les données contre l'accès ou la copie par des tiers non autorisés et contre la destruction, l'altération ou la perte.

3.8 Conservation de données à la demande de l'agent compétent [13]

Outre l'obligation de conservation générale telle qu'expliquée dans le point précédent, il est également possible qu'un officier de police judiciaire ou un officier de renseignement ordonne à un opérateur ou fournisseur de services de conserver des données spécifiques.

Le receveur d'un tel ordre de conservation doit conserver les données indiquées pendant une période de 90 jours pouvant être prolongée par écrit.

[10] Art 126/1 §2 LCE
[11] Art 126 §4 7° LCE
[12] Art 9 AR Rétention des données
[13] Art 39ter et 39quater §4 CIC

Cette demande sera généralement posée à l'opérateur pour s'assurer qu'une autorité requérante étrangère obtienne satisfaction dès qu'elle transmet sa demande d'entraide internationale aux autorités belges.

3.9 Destruction ou anonymisation des données après conservation obligatoire [14]

Dès que le motif pour la conservation des données liées à des communications électroniques disparaît car la période prévue est écoulée, l'opérateur ou le fournisseur de services doit supprimer ou anonymiser les données en question comme prévu dans le principe de base décrit à l'article 122 LCE.

3.10 Obligation de fourniture d'informations concernant les services et leur protection [15]

Un opérateur ou fournisseur de services doit fournir à l'autorité requérante les informations concernant ses services et les possibilités d'y avoir accès dans un langage clair.

3.11 Obligation de collaboration pour avoir accès aux communications [16]

Un opérateur ou fournisseur de services doit, si l'on lui demande, apporter sa collaboration afin de pouvoir avoir accès aux communications électroniques.

3.12 Fourniture de données d'identification et de données concernant les services fournis

L'opérateur doit fournir à l'autorité requérante les informations concernant :

- L'identification des abonnés ou des utilisateurs de leurs services (données à caractère personnel, adresse, adresse de facturation, contrat...)
- L'identification du moyen de communications électroniques utilisé (par ex. IMEI, IMSI, IP, MAC...)
- L'identification des services auxquels une personne est abonnée ou qui sont habituellement utilisés par une personne

3.13 Fourniture de données de trafic et de localisation

L'opérateur doit fournir à l'autorité requérante les informations concernant :

- L'identification des abonnés ou des utilisateurs de leurs services (données à caractère personnel, adresse, adresse de facturation, contrat...)
- L'identification du moyen de communications électroniques utilisé (par ex. IMEI, IMSI, IP, MAC...)
- L'identification des services auxquels une personne est abonnée ou qui sont habituellement utilisés par une personne

[14] Art 122 et 126 §4 6° LCE
[15] Art 90quater §4 et art 88quater CIC
[16] Art 90quater §4 et art 88quater CIC

3.14 Obligation d'interception et de fourniture des données interceptées

Un opérateur ou fournisseur de services doit pouvoir transmettre en temps réel les données d'un service de communications électroniques donné dans un langage clair au système central d'interception du NTSU CTIF.

Pour ce faire, l'opérateur ou le fournisseur de services doit connecter son système au système central d'interception du NTSU CTIF. Cette intégration est effectuée en concertation avec le NTSU CTIF. Dans ce cadre, il y a lieu de passer par DSU.NTSU.CTIF.IT@police.belgium.eu.

La même procédure doit être suivie à chaque fois que des modifications sont apportées à ce système.

L'opérateur reçoit de la permanence du NTSU CTIF les demandes des autorités compétentes accompagnées d'une fiche récapitulative des mesures demandées. Celles-ci doivent être exécutées immédiatement. En cas d'imprécisions ou de problème concernant l'exécution de la requête, l'opérateur est tenu de contacter DSU.NTSU.CTIF.PERM@police.belgium.eu ou de téléphoner au +32 2 642 77 11.

3.15 Synchronisation et précision des heures communiquées

Étant donné que le temps joue un rôle crucial dans les communications électroniques, il est absolument nécessaire que la configuration horaire de tous les systèmes impliqués se synchronise en permanence avec un signal fiable tel qu'une horloge atomique ou le signal GPS.

Si des heures doivent être communiquées pour les données de trafic, celles-ci seront exprimées jusqu'à la seconde.

3.16 Obligation de secret

Toute personne chez un opérateur requis qui prend connaissance de la demande et des données qui constituent la réponse est soumise au secret professionnel.

Cela signifie qu'elle ne peut communiquer aucune information concernant la requête, l'autorité requérante, la demande, la personne concernée, les éléments de la demande, la réponse ou quelque autre information concernant la requête à d'autres personnes que celles appartenant à la CCJ.

S'il est fait appel à des techniciens pour pouvoir satisfaire à la demande, cela a lieu sous la responsabilité de la CCJ et seules les informations strictement nécessaires sont communiquées aux techniciens en question.

Ces techniciens sont également tenus de respecter l'obligation de secret.

4 Dispositions pénales

4.1 Faire disparaître, détruire ou altérer des données dont la conservation a été demandée

Si une personne à qui il a été demandé de conserver des données fait disparaître, détruit ou altère ces données, celle-ci est passible d'un emprisonnement de six mois à un an et d'une amende de 26 euros à 20 000 euros, ou d'une de ces peines seulement.

4.2 Non-respect de l'obligation de conservation imposée par la loi[17]

En cas de non-respect de l'obligation de conservation prévue, la LCE prévoit des amendes pouvant atteindre 50 000 euros.

4.3 Refus de collaborer ou pas de collaboration dans le délai demandé

En fonction de la collaboration demandée, ne pas apporter la collaboration légalement requise est punissable d'amendes ou d'emprisonnement.
De même, ne pas fournir la collaboration demandée en temps réel ou dans le délai imparti par l'autorité compétente est puni de manière similaire.
Les amendes peuvent s'élever de 26 euros à 20 000 euros.
L'emprisonnement peut aller de six mois à un an.

4.4 Violation de l'obligation de secret

Toute violation de l'obligation de secret, par exemple en donnant accès à des tiers non autorisés ou en leur donnant toute information sur la collaboration demandée, les personnes, les lieux ou les moyens de communications visés est punie conformément à l'article 458 du Code pénal.

Dans ce contexte, les tiers non autorisés sont toute personne qui n'appartient pas à la Cellule de coordination.
Toutefois, il est permis de faire appel à des techniciens afin qu'ils assistent exceptionnellement les membres de la Cellule de coordination. Dès ce moment, ils tombent également sous l'obligation de secret.

Il est donc important d'informer suffisamment le personnel impliqué quant à cette obligation de secret.

[17] Art 126 et art 145 LCE

5 Indemnités de collaboration

5.1 Principes généraux concernant l'indemnisation des opérateurs et fournisseurs de services

L'annexe à l'AR obligation de collaboration en cas de demandes judiciaires définit les indemnités prévues pour la collaboration requise des opérateurs ou des fournisseurs de services.

Tous les investissements ou coûts opérationnels que les opérateurs ou fournisseurs de services doivent consentir pour fournir leur collaboration aux autorités compétentes, selon les modalités prescrites par la loi ou imposées par les autorités, sont à la charge de ces opérateurs ou fournisseurs de services.

Les autorités indemnisent uniquement 5 activités avec un tarif spécifique : interrogation des données historiques, demande des données de trafic ou de localisation en temps réel, consultation des données de pylône, demande de collaboration pour l'interception de communications et demande pour des requêtes spéciales.

5.2 Les services indemnisés spécifiques avec un tarif propre

Les demandes qui donnent lieu à une indemnité par service octroyé sont :

Point	Service	Compensation
Art 2 1°	Observation en temps réel	92 €
Art 2 2°	Observation de données historiques (rétro)	80 €
Art 2 3°	Observation dans un réseau (pylônes / points d'accès au réseau)	115 €
Art 2 4°	Interception de communications	140 €
Art 2 5°	Demandes spécifiques Voir définition à l'article 1 de l'annexe	Coûts réels après présentation de pièces justificatives

Chaque opérateur ou fournisseur de services qui réalise sur demande l'un des services ci-dessus est indemnisé conformément à ce tarif.

5.3 Demandes spécifiques

Par demande spécifique, visée à l'article 2, 5°, il convient d'entendre une demande exceptionnelle non mentionnée sous un autre point de la présente annexe et qui présente une telle forme de complexité établie que l'opérateur d'un réseau de communications électroniques ou le fournisseur de service de communications électroniques ne peut y répondre automatiquement, mais uniquement en faisant intervenir un ou plusieurs experts techniques.

Par demande spécifique, l'on n'entend donc pas la demande de services qui tombent sous les catégories de services dotés d'un tarif spécifique ou de services au sein du forfait.
Pour ces services, les opérateurs et fournisseurs de services sont censés avoir optimisé leur fonctionnement afin de pouvoir rapidement fournir les informations ou le service requis à l'autorité de sorte que l'intervention de techniciens soit superflue.

5.4 Autres services couverts par un forfait

Afin de faciliter le traitement des demandes de collaboration et surtout de simplifier la facturation des services, tous les services qui étaient dans la régulation tarifaire valable de 2013 à 2016, et pour lesquels aucun tarif spécifique n'était prévu, tombent sous l'indemnité forfaitaire.

Les services couverts par l'indemnité forfaitaire sont donc les suivants :

Fourniture d'une copie du contrat
Fourniture d'une copie d'une facture
Fourniture d'une carte de couverture
Fourniture de données d'identification sur la base d'un MSISDN
Fourniture des services achetés par une personne
Fourniture des services achetés à une adresse
Fourniture des données IMEI-track (quels IMSI ont été couplés à cet IMEI)
Fourniture des données IMSI-track (quels IMEI ont été couplés à cet IMSI)
Fourniture de données d'identification de l'adresse IP d'un utilisateur à un moment donné
Communication d'une adresse IP attribuée à un utilisateur à un moment/une période donné(e)
Operator service track
Fourniture d'informations sur un point de vente d'une carte SIM
Fourniture d'un code PUK pour un(e) SIM - MSISDN donné(e)
Exécution de la réinitialisation d'une boîte de messagerie vocale couplée à un MSISDN
Fourniture d'informations concernant le rechargement d'une carte prépayée
Fourniture d'informations sur le mode de paiement d'un appel à partir d'une cabine téléphonique

5.5 Distinction entre grands et petits opérateurs

L'AR obligation de collaboration en cas de demandes judiciaires effectue une distinction entre les grands et petits opérateurs et fournisseurs de services.

Un grand opérateur / fournisseur de services est une partie qui doit traiter plus de 4 % du nombre annuel de demandes de collaboration pour lesquelles aucun tarif spécifique n'est prévu.

Tous les autres opérateurs tombent sous la réglementation pour les petits opérateurs en ce qui concerne l'indemnisation de services non spécifiques.

5.6 Les services indemnisés à partir d'un forfait annuel pour les grands opérateurs

Tous les autres services qui n'ont pas de tarif propre et ne sont pas considérés comme des demandes spécifiques qui sont réalisés par les grands opérateurs à la demande des autorités judiciaires sont indemnisés via un forfait annuel.

Ce forfait et sa répartition sont définis annuellement par AR.

Pour 2017 et 2018, ce forfait est fixé à 1,3 million d'euros.

La distribution de ce forfait est soumise à une clé de répartition qui sera basée sur une moyenne glissante de 5 ans des 5 plus grandes opérations en termes de montants. [18]

Actuellement, seuls Proximus, Telenet et Orange sont considérés comme des grands opérateurs. Aucun autre opérateur ou fournisseur de services ne dépasse la barre des 4 %.

5.7 L'indemnisation des petits opérateurs

Pour les services fournis aux autorités judiciaires, les petits opérateurs peuvent recevoir une indemnité annuelle de 1000 € si :

- Ils ont communiqué les informations de leur Cellule de coordination à l'IBPT
- Ils se sont engagés et préparés à l'utilisation de la plateforme d'échange TANK

6 Rôle du NTSU CTIF

Les articles 46bis et 88bis du CIC indiquent que les autorités peuvent non seulement adresser leurs demandes directement aux opérateurs et fournisseurs de services, mais elles peuvent également le faire par le biais du service de police désigné par le Roi.

Les articles 1, 3 et 10bis de l'AR obligation de collaboration en cas de demandes judiciaires désignent le NTSU CTIF comme étant ce service.

Les articles 3, 4, 5 et 6 de l'AR obligation de collaboration services de renseignement prévoient que le dirigeant d'un service de renseignement peut définir la manière dont les informations doivent être fournies.

Depuis 2003, le NTSU CTIF est le gestionnaire du système central d'interception dans le cadre d'enquêtes judiciaires. Depuis 2010, l'infrastructure CTIF est également utilisée pour les interceptions effectuées à la demande des services de renseignement.

Le NTSU CTIF mènera le projet TANK, le mettra en œuvre et gérera la plateforme d'échange.

	Disponibilité	Coordonnées
Permanence CTIF	24/7 via tél.	02 642 77 11 DSU.NTSU.CTIF.PERM@police.belgium.eu
Permanence TIC CTIF	24/7 uniquement via perm CTIF	DSU.NTSU.CTIF.IT@police.belgium.eu

7 Compétence de régulation des autorités en matière d'échange des données

Conformément à l'article 10bis de l'AR obligation de collaboration en cas de demandes judiciaires et à l'article 6 de l'AR obligation de collaboration services de renseignement, les autorités ont la possibilité de définir la manière et le format de l'échange des données.

Conformément à l'article 6 de l'AR obligation de collaboration en cas de demandes judiciaires et à l'article 10 AR obligation de collaboration services de renseignement, les autorités ont la possibilité

[18] Étant donné que ces services n'ont plus de tarifs propres, la clé de répartition est calculée sur la base du tarif qui était valable de 2013 à 2016.

de choisir des options au sein des normes ETSI et 3GPP afin de standardiser le format et le transfert de données.

8 Projet Tank

8.1 Description générale du projet

Le projet TANK 2.0 prévoit le développement d'un échange automatisé de demandes et de réponses entre la police et les services de renseignement, d'une part, et les opérateurs et les fournisseurs de services, d'autre part.

Les utilisateurs de la police ou des services de renseignement pourront, conformément à une demande de l'autorité compétente, introduire des demandes et ajouter les requêtes y afférentes dans un site web interne, disponible dans leur environnement de travail ordinaire. Ils pourront également télécharger les données à partir de celui-ci, dès qu'elles seront disponibles.

Une fois la demande introduite, celle-ci est traitée par TANK, associée à un numéro unique et formatée en un format numérique spécifique.

Les opérateurs pourront extraire la demande du serveur web TANK ou la recevoir via les services web. Après le traitement, les opérateurs pourront placer leur réponse sur leur même serveur web ou la transmettre via les services web.

Les opérateurs et fournisseurs de services qui travaillent via le serveur web TANK seront prévenus par mail à chaque fois qu'une nouvelle demande est disponible.

TANK s'efforcera d'automatiser un nombre maximum de demandes types, ainsi que les demandes d'observation en temps réel et les demandes d'interception. Les informations en réponse à ces demandes seront envoyées par l'opérateur concerné au système central d'interception des autorités.

L'enregistrement des demandes et des réponses dans TANK constituera la base pour le soutien du paiement des services avec un tarif spécifique, d'une part, et pour le calcul de la clé de répartition du forfait annuel pour les grands opérateurs, d'autre part.

8.2 Architecture

L'architecture de la plateforme d'échange sera fixée de manière définitive au cours de la phase de développement. Dans les grandes lignes, l'architecture de TANK est la suivante :

- Une base de données qui enregistre les demandes, les documents justificatifs et les réponses reçues.
  Les réponses sont conservées pendant un temps limité seulement, jusqu'à la vérification par le demandeur.
- Un serveur web avec application web pour les utilisateurs introduisant une demande
- Un serveur web avec application web pour les opérateurs
- Un serveur de messagerie qui envoie des messages à chaque fois que de nouvelles demandes sont disponibles
- Une plateforme de services web pour un échange crypté entièrement automatique de demandes et de réponses entre TANK et les opérateurs complètement intégrés

8.3 Définition des formats de réponse standard

Afin de mettre un terme aux différents formats de réponse utilisés actuellement par les opérateurs et les fournisseurs de services, le projet consistera en premier lieu à définir un format de réponse fixe pour les différents types de demandes. Ce format devra être respecté quel que soit l'opérateur ou le fournisseur de services.

8.4 Calendrier du projet

L'étude préliminaire de ce projet a été réalisée en 2016. Le développement du projet débutera en mai 2017 et durera une année civile selon les estimations.

Le développement se déroulera en 2 phases :

Phase 1 : développement de la base de données, des applications web pour les utilisateurs et les opérateurs, des services mails et de l'automatisation des demandes en matière d'identification.
Réception prévue phase 1 : T4 2017.

Phase 2 : développement des services web pour l'échange automatisé avec les grands opérateurs, poursuite de l'automatisation d'autres demandes dont les demandes d'observation en temps réel et d'interception.
Réception prévue phase 2 : T2 2018.

8.5 Possibilités d'intégration avec TANK

Il est évident que le besoin d'intégration dans le système TANK dépendra du nombre de questions que les opérateurs devront traiter chaque année. Afin d'éviter une intégration coûteuse de TANK pour les petits opérateurs et de pouvoir engager immédiatement de nouveaux opérateurs dans le processus de fonctionnement des autorités, 2 options ont été prévues en matière d'intégration :

- « Light integration » : l'opérateur ou le fournisseur de services utilise uniquement l'application web et est averti par mail lorsqu'une nouvelle demande est arrivée.
- « Full integration » : pour chaque type de demande, il sera possible d'aboutir à un échange automatisé de demandes et de réponses sur la base de services web.

La « full integration » est d'abord uniquement prévue pour les grands opérateurs ou fournisseurs de services. Toutefois, si un petit opérateur ou fournisseur de services estime que le nombre de demandes qu'il doit traiter est suffisamment élevé pour passer à une « full integration » pour certains types de demandes, il devra transmettre sa requête au service NTSU CTIF qui décidera, après évaluation, si cette requête sera satisfaite.

En fonction du déroulement du développement, les demandes seront d'abord disponibles via l'application web. Les services web seront développés ensuite.

Les opérateurs ou fournisseurs de services travailleront donc via l'application web pour certains types de demandes et via les services web pour les autres demandes.

8.6 Obligations de collaboration concernant TANK

Bien que le cadre légal actuel prévoie une interrogation directe et une interrogation via un intermédiaire, le but des autorités est que toutes les demandes passent à terme par TANK. Dès que

TANK sera sur pied en tant que plateforme d'échange, les dispositions légales en question seront adaptées en ce sens.

Tous les opérateurs, qu'ils soient grands ou petits, seront donc à terme obligés de collaborer avec les autorités via la plateforme d'échange TANK.

Afin de pouvoir collaborer à l'aide de TANK, l'opérateur ou le fournisseur de services concerné devra effectuer au minimum les actions suivantes :

- Communiquer les coordonnées de la Cellule de coordination Justice et de ses membres
- Demander un avis de sécurité pour les membres de la CCJ
- Prévoir une adresse e-mail suivant la structure : TANK.CCJ@providername.extension
- Contrôler en permanence cette adresse e-mail pour prendre connaissance des nouvelles demandes
- Traiter les nouvelles demandes via l'application web dès réception d'un mail de notification
- Composer les réponses conformément au format défini par les autorités
- Les fichiers de réponse auront le format qui sera communiqué ultérieurement.
- Placer les réponses sur le serveur web TANK via l'application web

Pour les opérateurs qui veulent développer une « full integration », l'engagement va plus loin :

- Le développement d'applications intégrantes qui communiquent des services web avec TANK
- L'intégration avec le système central d'interception pour les demandes d'observation en temps réel et pour l'interception de communications électroniques

9 Engagement en vue d'obtenir l'indemnité forfaitaire annuelle en tant que petit opérateur

9.1 Identification de l'opérateur

Nom de la société	
Type d'opérateur	
Nature des services fournis	
Adresse	
Personne de contact	
Téléphone de contact	
E-mail de contact	
N° TVA	
Mandat signataire	

9.2 Inscription de la CCJ et coordonnées

Le soussigné confirme que la société ci-dessus :

- A pris connaissance des obligations et des conditions imposées par la loi aux opérateurs et aux fournisseurs de services ;
- A mis sur pied une CCJ dont les coordonnées ont été communiquées à l'IBPT ;
- A introduit une demande d'avis de sécurité pour les membres de la CCJ ;
- A pris les dispositions nécessaires pour satisfaire aux obligations légales.

9.3 Nomination d'un préposé à la protection des données à caractère personnel

Le soussigné confirme que la société ci-dessus :

- A nommé un préposé à la protection des données à caractère personnel
- A communiqué les coordonnées de ce préposé à la Commission de la protection de la vie privée

9.4 Engagement de collaboration via la plateforme TANK

Le soussigné confirme que la société ci-dessus :

- A pris connaissance des informations concernant le projet TANK et les principes pour l'échange de données avec les autorités compétentes dans le cadre de demandes et réponses
- S'engage à adapter le fonctionnement de sa CCJ à l'utilisation de la plateforme d'échange TANK dès que celle-ci sera disponible et fournira les réponses au format tel que défini par les autorités.

9.5 Demande d'indemnité en tant que petit opérateur

Le soussigné soumet, conformément à l'article 3 de l'annexe à l'AR obligation de collaboration, la demande d'indemnité en tant que petit opérateur

Fait à …….. le ……/……/2017 Signature