

Tilburg University

L'échange d'informations: Precis

Spapens, Antonius; Mouris, Melina; Ourahma, Samir; van Hout, Diana; Öner, Cihat

Publication date:
2022

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):

Spapens, A., Mouris, M., Ourahma, S., van Hout, D., & Öner, C. (2022). *L'échange d'informations: Precis: L'échange d'informations en matière de droit pénal, administratif et fiscal dans le cadre de la lutte contre la criminalité transfrontalière au sein de l'Euregio Meuse-Rhin*. Tilburg University.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

L'ÉCHANGE D'INFORMATIONS : PRECIS

L'échange d'informations en matière de droit pénal, administratif et fiscal dans le cadre de la lutte contre la criminalité transfrontalière au sein de l'Euregio Meuse-Rhin

Toine Spapens, Melina Mouris, Samir Ourahma, Diana van Hout, Cihat Öner

Avec la collaboration de Itai Ben Avi

Rapport du 29 novembre 2021

Table des matieres

1	Introduction	3
1.1	Esquisse du cadre de travail	3
1.2	Délimitation du champ d'application du précis	3
1.3	Structure du précis	4
2	Les instruments d'échange transfrontalier d'informations	5
2.1	Introduction	5
2.2	Les instruments de l'échange d'informations en matière pénale	5
2.2.1	Dispositions au niveau de l'UE	5
2.2.2	Instruments multilatéraux pertinents pour la Belgique, l'Allemagne et les Pays-Bas	10
2.2.3	Instruments bilatéraux	11
2.3	Les instruments d'échange d'informations fiscales	13
2.3.1	Dispositions multilatérales et au niveau de l'UE	13
2.3.2	Dispositions bilatérales	17
2.4	Les instruments d'échange d'informations sur la répression administrative	19
2.4.1	Cadres au niveau de l'UE	19
2.4.2	Cadres juridiques bilatéraux	22
2.5	Échange direct de renseignements en diagonale	23
3	Les cadres juridiques nationaux	24
3.1	Introduction	24
3.2	Les cadres juridiques nationaux en Belgique	24
3.2.1	Échange international d'informations en matière pénale	24
3.2.2	Échange international de renseignements fiscaux	27
3.2.3	Échange international d'informations administratives	28
3.3	Les cadres juridiques nationaux en Allemagne	29
3.3.1	Échange international d'informations en matière pénale	29
3.3.2	Échange international d'informations fiscales	34
3.3.3	Échange international d'informations administratives	36
3.4	Les cadres juridiques nationaux aux Pays-Bas	36
3.4.1	Échange international d'informations en matière pénale	36
3.4.2	Échange international d'informations fiscales	40
3.4.3	Échange international d'informations administratives	43
4	Échange de données au niveau national	44
4.1	Introduction	44
4.2	Les possibilités d'échange en Belgique	44
4.2.1	Fourniture d'informations par la police	44
4.2.2	Transmission d'informations par le ministère public	45
4.2.3	Fourniture d'informations par les instances administratives	46
4.2.4	Transmission d'informations par les autorités fiscales	46
4.2.5	Communication d'informations par les autorités douanières	46
4.3	Les possibilités d'échange en Allemagne	47
4.3.1	Fourniture d'informations par la police	47
4.3.2	Communication d'informations par le ministère public	49
4.3.3	Communication d'informations par les organes administratifs	50
4.3.4	Communication d'informations par l'administration fiscale	51
4.3.5	Communication d'informations par le Zollfahndungsdienst	51
4.4	Les possibilités d'échange aux Pays-Bas	52
4.4.1	Échanges au sein des centres régionaux d'information et d'expertise (CRIA)	52
4.4.2	Communication d'informations par la police et la Maréchaussée royale des Pays-Bas	53
4.4.3	Communication d'informations par le ministère public	53
4.4.4	Communication d'informations par les Communes et les provinces	54
4.4.5	Communication d'informations par l'administration fiscale	54
4.4.6	Communication d'informations par les douanes et la DGIF	55
5	Conclusion	56

1 Introduction

1.1 Esquisse du cadre de travail

Au cours des dernières décennies, l'Union européenne (UE) a connu un processus continu d'intégration économique et sociale. Ce processus s'accélère particulièrement lorsque le traité d'Amsterdam intègre l'acquis de Schengen dans le cadre juridique de l'UE en 1997. Cela signifie un élargissement de l'espace Schengen, où il n'y a plus de contrôles permanents aux frontières et où la libre circulation des personnes, des biens et des capitaux devient possible. En 1995, l'accord de Schengen entre en vigueur dans les cinq pays de l'espace Schengen initial : Belgique, Allemagne, France, Luxembourg et Pays-Bas. Les trois pays du Benelux bénéficient déjà de cette libre circulation depuis 1962. Les pays concernés comprennent que la libre circulation comporte aussi des risques. Les criminels peuvent plus facilement profiter de l'absence de contrôles aux frontières, par exemple pour passer des stupéfiants en contrebande, commettre des délits financiers de l'autre côté de la frontière ou réaliser des opérations criminelles plus complexes, comme la production de drogues synthétiques, à travers les zones frontalières.¹

Les régions frontalières, en particulier celles qui présentent un niveau élevé de cohésion sociale et économique, associé ou non à un degré élevé d'urbanisation, sont en moyenne plus exposées aux effets de la criminalité transfrontalière. Les autorités de ces régions frontalières sont donc souvent les premières à chercher des moyens d'améliorer la coopération en matière de lutte contre cette criminalité et font office de « laboratoires », dont les expériences sont ensuite intégrées aux systèmes juridiques au niveau national, voire européen.² Le programme EMR-EYES peut être considéré comme un ajout récent à une palette d'initiatives.

L'objectif à court terme du programme EMR-EYES est de promouvoir l'échange de données entre les autorités qui jouent les rôles les plus importants dans la lutte contre la grande criminalité organisée dans la zone frontalière. À moyen et long terme, l'objectif est de parvenir à une plus grande harmonisation des lois et réglementations dans les trois pays concernés. Outre la coopération pénale et policière, l'accent est également mis sur les contributions que les services administratifs et fiscaux, tels que les douanes et l'administration fiscale, peuvent apporter à la lutte contre la criminalité transfrontalière. La volonté d'adopter une approche multidisciplinaire (intégrée) des problèmes de criminalité entraîne un besoin important d'échange d'informations entre les organismes susmentionnés, tant au niveau national qu'international.

Ce précis donne un aperçu des cadres juridiques de l'échange transfrontalier d'informations entre les autorités (répressives ou non) pénales, administratives et fiscales de l'Euregio Meuse-Rhin. Il s'agit avant tout de l'échange d'informations entre les autorités ayant des compétences similaires. Dans un second temps, ce précis aborde les possibilités d'échange de données entre les autorités susmentionnées, au niveau national.

1.2 Délimitation du champ d'application du précis

Le précis se concentre sur l'échange d'informations. Il est donc nécessaire de définir soigneusement ce que l'on entend par là et quels sont les cadres juridiques qui font et ne font pas l'objet de ce précis.

Une première délimitation du concept d'information, tel qu'il est utilisé dans le précis, est **qu'il doit s'agir de données écrites ou enregistrées numériquement dont l'autorité dispose déjà d'office et dont la collecte ne requiert aucun pouvoir d'enquête, de contrôle ou de surveillance**. Ce dernier point dépasse le cadre de ce précis. Toutefois, ce précis aborde, par exemple, les scans d'informations écrites ainsi que les empreintes digitales ou les profils ADN stockés dans des bases de données.

Deuxièmement, il faut faire une distinction entre l'échange formel et informel d'informations. Les informations échangées lors d'une consultation entre les autorités concernées sont considérées comme informelles. **Les cadres juridiques ne couvrent que l'échange formel d'informations, en ce compris les informations de la police. Le précis se limite donc à cela.**

¹ C. Fijnaut (2019). A Peaceful Revolution. The Development of Police and Judicial Cooperation in the European Union. Intersentia.

² C. Fijnaut & T. Spapens (2010). The Meuse-Rhine Euregio: A Laboratory for Police and Judicial Cooperation in the European Union dans F. Lemieux(ed) International Police Cooperation. Emerging Issues, Theory and Practice (p. 101-125). Willan Publishing.

Troisièmement, le précis traite de l'échange **d'informations au sein de l'Euregio Meuse-Rhin**. Naturellement, l'échange d'informations avec d'autres pays, tant à l'intérieur qu'à l'extérieur de l'UE, peut également être nécessaire lorsque des activités criminelles le justifient. Dans une mesure plus ou moins grande, d'autres cadres juridiques et possibilités s'appliquent à l'échange d'informations avec les autres États membres et certainement avec les pays tiers.

Quatrièmement, les informations sont échangées de diverses manières. Tout d'abord, il est possible de donner des informations par écrit sous la forme d'un rapport officiel ou d'un autre document officiel et de les transférer ensuite, ou d'envoyer des documents originaux saisis à une occasion antérieure. En outre, les informations peuvent être communiquées formellement par voie orale, par exemple dans des situations d'urgence. L'échange peut soit être confirmé ultérieurement par écrit par le pays émetteur, soit être enregistré directement dans un rapport ou un système d'enregistrement, par le pays récepteur. En outre, au sein de l'UE, divers systèmes d'information sont utilisés par les autorités chargées des enquêtes criminelles pour les données relatives aux personnes et aux objets, tels que les véhicules. Citons par exemple le système d'information Schengen et la base de données Prüm pour les traces ADN et dactyloscopiques, ainsi que les données d'immatriculation des véhicules, qui peuvent être consultées directement par les États membres. Une autre distinction peut être faite entre l'échange d'informations sur demande et l'échange d'informations spontané. Ce dernier point concerne souvent des données qui sont connues du pays fournisseur, mais qui peuvent ne pas être connues du pays récepteur. **Le précis contient les cadres juridiques de toutes ces formes d'échange d'informations.**

Enfin, les cadres juridiques relatifs à l'échange d'informations pénales et fiscales sont composés d'un large éventail d'instruments juridiques adoptés à des niveaux décisionnels divers, allant du niveau mondial au niveau bilatéral. D'une part, certaines dispositions de ces différents instruments sur l'échange d'informations sont très similaires parce que les traités plus récents ont adopté le libellé des traités antérieurs. D'autre part, un nouvel instrument peut offrir les mêmes possibilités qu'un traité existant, mais les élargir. **Ce précis traite des instruments les plus récents, et des instruments antérieurs uniquement dans la mesure où ils offrent des possibilités différentes.**

1.3 Structure du précis

Dans la suite de ce précis, le chapitre 2 présente tout d'abord le cadre juridique international de l'échange d'informations applicable à la Belgique, à l'Allemagne et aux Pays-Bas. Ensuite, le chapitre 3 traite de la question de savoir comment les différents instruments internationaux ont été mis en œuvre dans la législation nationale des trois pays. Le chapitre 4 traite des possibilités juridiques de la transmission d'informations par les autorités compétentes à des tiers dans leur propre pays.

2 Les instruments d'échange transfrontalier d'informations

2.1 Introduction

Ce chapitre examine les instruments européens et internationaux relatifs à l'échange transfrontalier d'informations, en ce qui concerne la Belgique, l'Allemagne et les Pays-Bas. Une distinction est faite entre les informations relevant du droit pénal (section 2.2), les informations relevant du droit fiscal (section 2.3) et les informations relevant du droit administratif (section 2.4).

2.2 Les instruments de l'échange d'informations en matière pénale

Les instruments d'échange d'informations en matière pénale consistent en un système de directives et de décisions-cadres de l'UE, de traités multilatéraux conclus en dehors du cadre de l'UE et de traités bilatéraux entre les trois pays couverts par ce vade-mecum.³ Dans ces cadres, une autre distinction peut être faite entre l'échange de données policières, c'est-à-dire les informations détenues par les autorités chargées des enquêtes, et les données judiciaires, qui sont des informations relatives aux affaires pénales et aux condamnations.

2.2.1 Dispositions au niveau de l'UE

Échange de données de police

Au niveau de l'UE, le principal instrument régissant l'échange de données policières est la Décision-cadre 2006/960/JAI, également connue sous le nom de décision-cadre suédoise.⁴ La décision-cadre couvre l'échange d'informations et de renseignements à des fins d'enquête, mais ceux-ci ne peuvent être utilisés comme preuves dans une procédure pénale sans le consentement de l'intéressé. Une demande doit être faite par l'autorité compétente en vertu du droit national et par les méthodes de communication déterminées au niveau national. Ce consentement n'est pas requis si l'État membre dont la transmission d'information est requise a déjà donné son accord à l'utilisation d'informations comme preuves au moment de la transmission des informations ou des renseignements (art. 1, al. 4). La décision-cadre n'impose aucune obligation d'obtenir des informations ou des renseignements au moyen de mesures coercitives, définies conformément au droit national, dans l'État membre ou le pays tiers qui reçoit la demande d'informations ou de renseignements (art. 1, al. 5). Les informations et les renseignements obtenus précédemment au moyen de mesures coercitives sont fournis par les États membres dans la mesure où le droit national le permet et conformément à celui-ci (art. 1, al. 6). En outre, elle n'affecte pas l'obligation de respecter les droits fondamentaux et les principes juridiques fondamentaux tels qu'ils sont consacrés par l'article 6 du Traité sur l'Union européenne, et aucune obligation incombant à cet égard aux services répressifs n'est affectée (art. 1, al. 7).

Les informations peuvent être échangées par un service répressif compétent, autorisé par le droit national à dépister, prévenir et enquêter sur des infractions ou des activités criminelles, et à exercer son autorité et à prendre des mesures coercitives dans le cadre de ces activités. Les agences ou unités spécialisées dans les questions de sécurité nationale ne relèvent pas de la notion de service répressif compétent (art. 2, al.a). Il appartient aux États membres de déterminer quelles autorités sont considérées comme des services répressifs.

La décision-cadre couvre à la fois les enquêtes criminelles et les opérations de renseignement criminel. L'enquête pénale est la phase procédurale au cours de laquelle des mesures sont prises par les services répressifs ou judiciaires compétents, y compris les parquets, pour identifier et établir les faits, les suspects et les circonstances ayant trait à un ou plusieurs actes criminels concrets (art. 2, al. b). Par opération de renseignement en matière pénale, on entend une étape procédurale, qui n'a pas encore atteint le stade de l'enquête pénale, au sein de laquelle un service répressif compétent est autorisé par le droit national à recueillir, traiter et analyser des informations sur la criminalité ou des activités criminelles en vue d'établir si des actes

³ Les traités du Benelux, bien que formellement trilatéraux, sont décrits ici comme bilatéraux entre la Belgique et les Pays-Bas.

⁴ Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne. Journal officiel de l'Union européenne. L386/89.

criminels précis ont été commis ou pourraient l'être (art. 2, al. c). Les informations et/ou les renseignements couvrent tout type d'informations ou de données détenues par les services répressifs, ainsi que les informations ou les données détenues par des autorités publiques ou des entités privées et dont les services répressifs peuvent disposer sans prendre de mesures coercitives, conformément à l'article 1er, paragraphe 5 (art. 2, al. d). La possibilité d'échanger des informations et des renseignements est limitée par le fait qu'il doit s'agir d'infractions telles que définies à l'article 2, alinéa 2, de la Décision-cadre 2002/584/JAI du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, ou d'infractions qui correspondent ou sont équivalentes, selon le droit national, à celles définies dans cette disposition (art. 2, al. e).⁵

La décision-cadre établit une distinction entre l'échange à la demande et l'échange spontané. Les informations et les renseignements sont fournis à la demande d'un service répressif compétent, agissant dans le cadre des compétences qui lui sont conférées par le droit national, qui mène une enquête en matière pénale ou une opération de renseignement en matière pénale (art. 3, al. 2). La transmission d'informations et de renseignements ne doit pas être soumise à des conditions plus strictes que celles prévues au niveau national (art. 3, al. 3). Des informations et des renseignements aux fins de dépistage et de prévention d'une infraction ou dans le cadre d'une enquête en la matière peuvent être demandés s'il existe des raisons factuelles de croire que des informations et des renseignements pertinents sont disponibles dans d'autres États membres. La demande doit indiquer ces raisons factuelles, les fins dans lesquelles les informations et les renseignements sont sollicités et le lien entre ces fins et la personne à laquelle l'information et le renseignement se rapportent (art. 5, al. 1). À titre de restriction, le service répressif compétent requérant s'abstient de demander plus d'informations ou de renseignements, qu'il n'est nécessaire aux fins de la demande (art. 5, al. 2).

Les services répressifs compétents peuvent fournir des informations et des renseignements sans demande préalable, lorsqu'il existe des raisons factuelles de penser que ces informations et renseignements pourraient contribuer au dépistage, à la prévention ou à l'enquête des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI (art. 7, al. 1). Les modalités d'un tel échange spontané d'informations sont régies par le droit national des États membres qui fournissent les informations. La communication d'informations et de renseignements est limitée à ce qui est jugé pertinent et nécessaire pour le dépistage, la prévention du délit ou de l'activité délictueuse en question ou l'enquête à son sujet (art. 7, al. 2).

La décision-cadre contient plusieurs motifs de refus. L'échange peut être refusé lorsqu'il porterait atteinte aux intérêts vitaux de l'État membre requis en matière de sécurité nationale, nuirait au bon déroulement d'une enquête en cours ou d'une opération de renseignement en matière pénale ou à la sécurité des personnes, ou serait manifestement disproportionné ou non pertinent au regard des finalités pour lesquelles il a été demandé (art. 10, al. 1). Lorsque la demande concerne une infraction passible d'une peine d'emprisonnement d'un an ou moins selon le droit de l'État membre requis, la communication des informations ou des renseignements demandés peut également être refusée (art. 10, al. 2).

Il est important que les informations et les renseignements puissent être échangés par tous les canaux existants de coopération internationale en matière de répression. En cas d'urgence, les demandes peuvent être échangées via des points de contact préétablis désignés par les États membres (art. 6, al. 1). En outre, la décision-cadre contient des normes sur le délai de réponse aux demandes régulières ainsi qu'un formulaire standard pour soumettre une demande.

En ce qui concerne les relations avec d'autres instruments juridiques, la décision-cadre indique que les États membres peuvent continuer à appliquer les conventions ou accords bilatéraux ou multilatéraux en vigueur au moment de l'adoption de la décision-cadre, dans la mesure où ces accords ou arrangements permettent d'étendre ou d'élargir les objectifs de la décision-cadre et contribuent à simplifier ou à faciliter davantage les procédures d'échange d'informations et de renseignements relevant du champ d'application de la décision-cadre (art. 12, al. 3). Il en va de même pour les nouveaux instruments (art. 12, al. 4).

La décision-cadre suédoise fournit donc un large cadre pour l'échange de données policières, mais aussi diverses possibilités pour les États membres de soumettre cet échange à des restrictions spécifiques. Il sera examiné dans les chapitres suivants dans quelle mesure cela est le cas.

⁵ Décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (2002/584/JAI). Journal officiel des Communautés européennes. L190/1.

Le deuxième instrument au niveau de l'UE qui contient des dispositions sur l'échange de données policières est la Décision 2008/615/JAI, ou *décision de Prüm*.⁶ Cette décision est dérivée du traité multilatéral de Prüm, qui est également en vigueur en Belgique, en Allemagne et aux Pays-Bas.

Dans le domaine de l'échange d'informations, la décision contient des dispositions relatives aux conditions et à la procédure de transfert automatisé des profils ADN, des données dactyloscopiques et de certaines données nationales relatives à l'immatriculation des véhicules (art. 1er, al. a) ainsi que des dispositions relatives aux conditions de transmission de données en liaison avec des manifestations de grande envergure revêtant une dimension transfrontalière (art. 1er, al. b).

Les articles 2 à 11 prévoient la possibilité d'effectuer des recherches dans les bases de données de profils ADN et d'empreintes digitales de manière automatique et anonyme selon le principe « hit/no-hit ». Si un profil ou une empreinte digitale correspondant est disponible (un résultat positif), des informations supplémentaires, y compris des données personnelles, peuvent être demandées par le biais d'une demande d'entraide judiciaire.

L'article 12 La Décision de Prüm régit la consultation automatisée des données d'immatriculation des véhicules. Ces informations peuvent être échangées aux fins de la prévention et de l'enquête en matière d'infractions pénales, et dans le cadre du traitement d'autres infractions relevant de la compétence des tribunaux ou du ministère public de l'État membre effectuant la consultation, ainsi que dans le cadre du maintien de la sécurité publique. Ces données comprennent des données relatives aux propriétaires ou détenteurs, et des données relatives aux véhicules. Les recherches ne peuvent être effectuées que sur la base d'un numéro de châssis complet ou d'un numéro d'immatriculation complet. Les recherches ne peuvent être effectuées que dans le respect du droit national de l'État membre effectuant la recherche (art. 12, al. 1). Aux fins de cet échange d'informations, chaque État membre désigne un point de contact national (art. 12, al. 2).

Les articles 13 et 14 traitent de la transmission d'informations non personnelles et de données à caractère personnel en vue de maintenir l'ordre et la sécurité publics. À l'occasion de manifestations majeures ayant une dimension transfrontalière, les États membres se transmettent, tant sur demande que de leur propre initiative, dans le respect du droit national de l'État membre qui transmet les données, les données à caractère non personnel qui peuvent être nécessaires à cet effet (art. 13). Dans le même contexte, l'article 14 prévoit la communication de données à caractère personnel si des condamnations graves ou d'autres circonstances font présumer que les personnes concernées commettront des infractions pénales au cours des manifestations ou présenteront un danger pour l'ordre et la sécurité publics, pour autant que la transmission de ces données soit autorisée en vertu du droit national de l'État membre qui transmet les données (art. 14, al. 1). Les données à caractère personnel ne peuvent être traitées qu'aux fins visées à l'alinéa 1 et pour les manifestations précises en vue desquelles elles ont été communiquées. Les données transmises doivent être effacées immédiatement, dès lors que les objectifs visés à l'alinéa 1 ont été atteints ou ne sont plus réalisables. En tout état de cause, les données transmises doivent être effacées après un an au plus tard (art. 14, al.2).

Le *système d'information Schengen* est un système d'alerte centralisé pour l'espace Schengen concernant, entre autres, les suspects recherchés et les personnes condamnées, dont les États membres ont une copie synchronisée (N.SIS). Il est utilisé à des fins criminelles, mais dans la pratique, principalement à des fins de migration. Le SIS contient, entre autres, de nombreux signalements de passeports volés et perdus. Un signalement, émis par un État membre, est « un ensemble de données introduites dans le SIS II pour permettre aux autorités compétentes d'identifier une personne ou un objet en vue de tenir une conduite particulière à son égard » (Décision 2007/533/JAI, art. 3, al 1 a).⁷ Une instruction pour une action concrète, telle qu'une arrestation ou une saisie, doit alors être donnée lorsque le système fournit une correspondance.

Dans chaque État membre, une agence N.SIS assume la responsabilité centrale du bon fonctionnement et de la sécurité du système, de l'accès des autorités compétentes et du respect de la décision. En outre, dans chaque État membre, il existe un bureau SIRENE qui contrôle la qualité des informations introduites dans le système et veille à ce que toutes les informations supplémentaires soient échangées conformément aux règles. Des informations supplémentaires peuvent être demandées aux autorités nationales 24 heures sur 24.

6 Décision du Conseil 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière. Journal officiel de l'Union européenne. L210/1.

7 Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II). Journal officiel de l'Union européenne. L205/63.

Relativement aux personnes faisant l'objet d'un signalement, il est au minimum enregistrés le nom, le sexe, une référence à la décision qui est à l'origine du signalement (Décision, art. 23 al. 1). En outre, un certain nombre d'autres données peuvent être enregistrées (Décision, art. 20, al. 3), notamment des photographies et des empreintes digitales. Si des photographies, des empreintes digitales et d'autres données sont disponibles, elles doivent être ajoutées pour faciliter l'identification. L'État membre signalant est responsable de l'exactitude et de l'actualité des données et est seul habilité à modifier, compléter, rectifier, mettre à jour ou effacer les données qu'il a introduites (art. 49, al. 1 et 2). Si un État membre autre que l'État membre signalant dispose d'indices faisant présumer qu'une donnée est entachée d'erreur de fait, il en informe l'État membre signalant, par voie d'échange d'informations supplémentaires, dans les meilleurs délais après avoir relevé ces éléments. L'État membre signalant vérifie ce qui lui est communiqué et, le cas échéant, corrige ou efface la donnée sans délai (art. 49, al. 3). Si une personne prétend ne pas être la personne recherchée au moyen d'un signalement, les États membres échangent des informations supplémentaires (al. 5).

Échange de données judiciaires

L'échange de données judiciaires a été traité pour la première fois dans un contexte multilatéral par la Convention européenne d'entraide judiciaire en matière pénale, adoptée par le Conseil de l'Europe en 1959. Au niveau de l'UE, les dispositions relatives à l'entraide judiciaire ont été fixées en 2000 dans la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (2000/C 197/01). L'article 7 de cette convention permet l'échange spontané d'informations en plus de la possibilité préexistante d'échanger sur la base d'une demande. Le mandat européen d'obtention de preuves (2008/978/JAI) a rendu le principe de reconnaissance mutuelle applicable, entre autres, aux documents et données destinés à être utilisés dans le cadre de procédures pénales.⁸ Toutefois, cette Décision-cadre se limitait aux preuves déjà existantes. En ce qui concerne les États membres de l'UE, ces instruments ont été remplacés en 2014 par la décision d'enquête européenne.⁹

Décision d'enquête européenne (DEE)

La décision d'enquête européenne (DEE) permet aux autorités judiciaires de demander plus facilement des preuves (au sens large) à un autre pays de l'UE, y compris des preuves déjà en possession des autorités compétentes de l'État d'exécution (art. 1, al. 1). Une décision d'enquête européenne peut être émise par un juge, une juridiction, un juge d'instruction ou un procureur compétent dans l'affaire, ou toute autre autorité compétente désignée par l'État d'émission, agissant en tant qu'autorité chargée de l'enquête pénale dans l'affaire en question et habilitée à ordonner la collecte de preuves conformément au droit national (art. 2).

Une décision d'instruction européenne peut être émise dans le cadre de procédures pénales engagées ou susceptibles d'être engagées par ou devant une autorité judiciaire pour des faits punissables selon le droit national de l'État d'émission ; dans le cadre de procédures engagées par une autorité administrative pour des faits punissables selon le droit national de l'État d'émission en raison de leur caractère d'infraction aux règles de droit, à condition que la décision puisse donner lieu à un recours devant une juridiction compétente, notamment en matière pénale ; dans le cadre d'une procédure engagée par une autorité judiciaire pour des faits qui sont punissables selon le droit national de l'État d'émission en raison de leur caractère d'infraction aux règles de droit, et lorsque la décision peut donner lieu à une procédure devant une juridiction compétente notamment en matière pénale, ainsi que dans le cadre des procédures susmentionnées relatives à une infraction ou à un manquement aux règles de droit pouvant engager la responsabilité d'une personne morale ou entraîner une peine à son encontre dans l'État d'émission (art. 4).

La DEE contient quelques dispositions spécifiques sur l'obtention d'informations relatives aux comptes bancaires et autres comptes financiers (art. 26) et aux opérations bancaires et autres opérations financières (art. 27). Une ordonnance peut être rendue pour déterminer si une personne physique ou morale faisant l'objet d'une procédure pénale détient ou contrôle un ou plusieurs comptes de toute nature dans une banque située sur le territoire de l'État d'exécution. Dans ce cas, les détails complets des comptes identifiés peuvent être demandés. Les données peuvent également concerner des comptes pour lesquels la personne faisant l'objet de la procédure pénale dispose d'une procuration. En outre, le mandat peut être émis afin de vérifier si une

8 Décision-cadre 2008/978/JAI du Conseil du 18 décembre 2008 relative au mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales. Journal officiel de l'Union européenne. L350/72.

9 Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale. Journal officiel de l'Union européenne. L130/1.

personne physique ou morale faisant l'objet de la procédure pénale concernée détient un ou plusieurs comptes dans une institution financière non bancaire sur le territoire de l'État d'exécution.

Une décision d'instruction européenne peut également être émise, conformément à l'article 27, afin d'obtenir les détails de comptes bancaires déterminés et d'opérations bancaires qui ont été effectuées pendant une période déterminée par l'intermédiaire d'un ou de plusieurs comptes bancaires, y compris les détails d'un compte d'origine ou de destination. L'obligation prévue par le présent article ne s'applique que dans la mesure où les données sont en possession de la banque où le compte est détenu. Dans ce cas, outre les motifs de refus de reconnaissance ou d'exécution prévus à l'article 11, l'exécution de la décision d'enquête européenne peut également être refusée si l'exécution de la mesure d'enquête ne serait pas autorisée dans le cadre d'une procédure nationale similaire.

L'article 11 contient un certain nombre de motifs de refus. Il est important, entre autres, que l'exécution puisse être refusée si la mesure d'instruction porte atteinte aux intérêts nationaux essentiels en matière de sécurité (art. 11, al.1b), ou si elle ne serait pas autorisée au titre du droit de l'État d'exécution dans le cadre d'une procédure nationale similaire (art. 11, al.1c).

Les données personnelles obtenues ne doivent être traitées que si elles sont nécessaires et proportionnées aux finalités compatibles avec la prévention, les enquêtes, la détection et la poursuite d'infractions pénales ou l'exécution de sanctions pénales et l'exercice des droits de la défense. Seules les personnes autorisées peuvent avoir accès aux informations contenant des données personnelles par le biais d'une procédure d'authentification (paragraphe 42 du préambule). L'article 19 dispose plus précisément que, conformément au droit national et sauf disposition contraire de l'autorité d'exécution, l'autorité d'émission veille à ce que les preuves ou les informations fournies par l'autorité d'exécution ne soient pas divulguées, sauf dans la mesure où leur divulgation est nécessaire aux fins des enquêtes ou des procédures précisées dans la décision d'enquête européenne (art. 19, al. 3). Les États membres doivent également prendre des mesures pour empêcher les banques de révéler aux clients concernés de la banque ou à d'autres tiers que des informations ont été transmises à l'État d'émission ou qu'une enquête est en cours (art. 19, al. 4).

Le *système européen d'information sur les casiers judiciaires ECRIS* est un système décentralisé contenant des informations sur les condamnations pénales des personnes, dans les États membres de l'UE (Décisions-Cadres 2009/315/JAI et 2009/316/JAI).¹⁰ Contrairement aux bases de données Prüm et au SIS, les États membres ne disposent pas d'un accès direct en ligne aux bases de données des autres États membres. Les États membres sont responsables de la mise à jour de leurs propres systèmes.

En vertu de l'article 4 de la décision-cadre 2009/315/JAI, les autorités centrales des États membres sont tenues d'informer le plus tôt possible les autorités centrales des autres États membres des condamnations pénales prononcées sur leur territoire à l'encontre de ressortissants desdits États membres (telles qu'inscrites dans le casier judiciaire national). Ce faisant, il est obligatoire de transmettre certaines informations (art. 11, al. 1a), notamment le nom, la date de naissance, le lieu de naissance, le sexe, la nationalité et, le cas échéant, les noms précédents. Les autres informations sont facultatives (uniquement si elles sont mentionnées dans le casier judiciaire) ou complémentaires (si elles sont accessibles). Cette dernière catégorie comprend le numéro d'identité de la personne condamnée, ou le type et le numéro de sa pièce d'identité, les empreintes digitales de la personne et, le cas échéant, les pseudonymes et/ou alias.

En vertu de l'article 6 de la Décision-Cadre 2009/315, l'autorité centrale d'un État membre peut demander des informations du casier judiciaire à l'autorité centrale d'un autre État membre aux fins d'une procédure pénale ou à toute autre fin. En vertu de l'article 8 de la décision-cadre, l'État-membre requis peut demander à l'État-membre requérant un complément d'information pour lui permettre d'identifier la personne visée par la demande. Cette demande de complément d'information prolonge le délai de réponse. En vertu de l'article 7, l'autorité centrale de l'État membre de la nationalité de la personne est tenue de fournir les informations si la demande concerne une procédure pénale. L'État membre requis n'est pas obligé de le faire si l'État membre requérant demande les informations pour une finalité différente, auquel cas le droit national prévaut.

¹⁰ Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 relative à l'organisation et au contenu de l'échange d'informations extraites du casier judiciaire entre les États membres. Journal officiel de l'Union européenne. L93/23 ; Décision 2009/316/JAI du Conseil du 6 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS) en application de l'article 11 de la décision-cadre 2009/315/JAI. Journal officiel de l'Union européenne. L93/33

Le Règlement (UE) 2019/816 a étendu le champ d'application de l'ECRIS pour y inclure ce qu'on appelle l'ECRIS-TCN, afin de permettre aux États membres de vérifier quels autres États membres détiennent des informations sur les casiers judiciaires des ressortissants de pays tiers condamnés dans l'Union par une juridiction pénale.¹¹

Enfin, il est important de mentionner la Directive 2016/680/UE sur la protection des données dans le cadre des enquêtes et des poursuites¹². Les principes généraux qui y sont énoncés sont par exemple : les données à caractère personnel doivent être traitées de manière licite et loyale, collectées de manière ciblée et proportionnée, et conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées (art. 4, al. 1). Le traitement par le même responsable ou par un responsable différent pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées est admissible si : le responsable est autorisé en vertu du droit de l'Union ou des États membres à traiter ces données à caractère personnel pour une telle finalité ; et si le traitement est nécessaire et proportionné à cette autre finalité en vertu du droit de l'Union ou des États membres (art. 4, al.2).

2.2.2 Instruments multilatéraux pertinents pour la Belgique, l'Allemagne et les Pays-Bas

La Belgique, l'Allemagne et les Pays-Bas sont parties à divers traités multilatéraux dont la législation européenne décrite ci-dessus reprend ou a repris les dispositions et qui ne sont donc plus directement pertinents. Nous ne traiterons ici que du Traité de 2005 entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale (ci-après : Traité de Prüm).

Le Traité de Prüm vise notamment à renforcer l'échange mutuel de données entre les pays participants. La majorité des dispositions du traité ont été reprises dans la législation européenne, par le biais de la décision de Prüm susmentionnée. Les exceptions sont les dispositions relatives à la migration illégale (chapitre 4) et certaines autres formes de coopération (chapitre 5).

L'article 26 du Traité concerne l'assistance en cas d'événements de grande envergure, de catastrophes et d'accidents graves. Les autorités compétentes des parties contractantes ont l'obligation de s'informer mutuellement, le plus tôt possible, de ces situations ayant des implications transfrontalières et d'échanger les informations pertinentes (art. 26, al. 1).

L'article 27 permet aux autorités compétentes des parties contractantes d'échanger directement des informations sur des questions spécifiques. Cet échange a lieu sur demande. Il s'agit de vérifier l'identité de propriétaires et de détenteurs ainsi que de conducteurs de véhicules routiers, de bateaux et navires ou d'aéronefs dans la mesure où cela ne peut être établi par une recherche automatisée dans les registres d'immatriculation des véhicules (art. 27, al. 2.1) ; de fournir des informations sur les permis de conduire, les permis de navigation et les autorisations semblables (art. 27, al. 2.2) ; d'établir les lieux de séjour et la résidence des personnes (art. 27, al. 2.3) ; d'établir les titres de séjour (art. 27, al. 2.4) ; d'établir l'identification des abonnés au téléphone et des abonnés à d'autres installations de télécommunication, dans la mesure où celles-ci sont accessibles au public (art. 27, al. 2.5) ; d'établir l'identification des personnes (art. 27, al. 2.6) ; de procéder à l'enquête sur la provenance d'objets tels que des armes, des véhicules à moteur et des bateaux (demande relative au canal de vente) (art. 27 al. 2.7) ; de transmettre les données du recueil de données policières et de documents de police ainsi que des informations provenant du recueil de données d'autorités administratives publiquement accessibles (art. 27, al. 2.8) ; les signalements urgents relatifs aux armes et explosifs ainsi que des signalements relatifs à la contrefaçon de moyens de paiement et de timbres (art. 27, al. 2.9) ; la transmission d'informations relatives à l'exécution pratique de mesures d'observation transfrontalières,

¹¹ Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 établissant un système centralisé permettant de déterminer quels États membres détiennent des informations sur les condamnations prononcées à l'encontre de ressortissants de pays tiers et d'apatrides (ECRIS-TCN), complétant le système européen d'information sur les casiers judiciaires et modifiant le règlement (UE) 2018/1726 Journal officiel de l'Union européenne. L135/1

¹² Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil Journal officiel de l'Union européenne L166/1.

de poursuites transfrontalières et de livraisons surveillées (art. 27, al. 2.10) ; et la notification de la disponibilité d'une personne à faire des déclarations (art. 27, al. 2.11). Si l'autorité requise n'est pas compétente pour le traitement de la demande, elle transmet la demande à l'autorité compétente. L'autorité requise informe l'autorité requérante de cette transmission et de l'autorité compétente pour le traitement de la demande. L'autorité compétente traite la demande et transmet le résultat à l'autorité requérante (art. 27, al. 3).

En outre, l'article 35 est important en ce qui concerne la finalité de l'utilisation. La partie contractante destinataire ne peut traiter les données à caractère personnel qu'aux fins pour lesquelles elles ont été fournies en vertu du traité ; le traitement à d'autres fins n'est admissible qu'après autorisation préalable de la Partie contractante gestionnaire des données et dans le respect du droit national de la Partie contractante destinataire. L'autorisation peut être délivrée pour autant que le droit national de la Partie contractante gestionnaire des données permette ce traitement à ces autres fins.

2.2.3 Instruments bilatéraux

La Belgique, l'Allemagne et les Pays-Bas ont conclu divers traités bilatéraux qui réglementent certains aspects spécifiques de l'échange d'informations. Deux traités seront examinés ci-après : le traité entre le Royaume des Pays-Bas, le Royaume de Belgique et le Grand-Duché de Luxembourg sur la coopération policière transfrontalière, conclu en 2004 (ci-après : le traité de Senningen) ; le traité entre le Royaume des Pays-Bas et la République fédérale d'Allemagne sur la coopération policière transfrontalière et la coopération en matière pénale (ci-après : le traité d'Enschede), également conclu en 2004. Aucun traité bilatéral de coopération policière ou pénale n'a été conclu entre la Belgique et l'Allemagne.

Échange de données de police

Le Traité de Senningen permet l'échange de données personnelles, la consultation directe des registres de véhicules et l'échange d'informations par l'intermédiaire d'officiers de liaison et dans des centres de police communs.

L'article 10 permet l'échange de données à caractère personnel « si cet échange est indispensable pour la bonne exécution des missions de police sur le territoire des Parties Contractantes, étant entendu que la transmission de données à caractère personnel à une autre Partie Contractante n'est possible que pour prévenir un danger grave et imminent ou pour rechercher un délit qui a affecté gravement l'ordre juridique de la Partie Contractante destinataire, à moins qu'il ne soit question d'une demande relative à une personne déterminée ou à un cas déterminé » (art. 10, al. 1).

L'échange de données personnelles est soumis à d'autres restrictions. Les données personnelles collectées peuvent être conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été collectées et traitées (art. 10, al. 3). Des restrictions s'appliquent également sur la base des articles 126 à 129 de la Convention d'application de l'Accord de Schengen (art. 10, al.2)¹³. L'article 126 traite du traitement automatisé des données à caractère personnel, c'est-à-dire des données transmises par le destinataire ou stockées par lui dans un système d'enregistrement. Les exigences pertinentes comprennent le fait que l'objectif doit être limité (art. 126, al. 3a). L'utilisation à d'autres fins est en principe possible, mais nécessite le consentement préalable du destinataire et est soumise à la législation nationale. L'article 129 permet également à la partie qui transmet des données d'imposer des conditions à l'utilisation des données personnelles transmises (art. 129, al. a). En outre, les données ne peuvent être utilisées que par les services, les organes et les autorités judiciaires qui ont une tâche ou une fonction en rapport avec les finalités susmentionnées (art. 126, al. 3b). La partie qui transmet les données doit s'assurer que les données transmises sont exactes (art. 126, al.3c). Enfin, l'article 126 stipule que tant la partie émettrice que la partie réceptrice doivent conserver un enregistrement des informations transmises ou reçues (art. 126, al. 3).

L'article 127 stipule que l'article précédent est également applicable à la transmission des données à caractère personnel provenant d'un fichier non automatisé et à l'intégration de ces données dans un fichier non automatisé (art 127, al. 1). Il existe toutefois quelques exceptions à cette règle, d'abord lorsqu'il s'agit d'« autres » cas et ensuite lorsque l'enregistrement « en vue de l'utilisation » n'est pas nécessaire, notamment

¹³ Cela fait référence à la : Convention d'application de l'Accord de Schengen du 14 juin 1985 entre le Royaume des Pays-Bas, le Royaume de Belgique, la République fédérale d'Allemagne, la République française et le Grand-Duché de Luxembourg relatif à la suppression graduelle des contrôles aux frontières communes ; Schengen, 19 juin 1990.

lorsque les données ne sont pas utilisées ou ne sont utilisées que très brièvement» (art. 127, al. 2a). Ce qu'il faut entendre exactement par « autres cas » ou par le terme « très brièvement » n'est pas précisé.

Dans le contexte de ce précis, il est important de noter que les articles 126 et 127 ne s'appliquent pas à l'entraide judiciaire en matière pénale (titre III, chapitre 2) ni au Système d'information Schengen (titre IV).

L'article 13 du Traité de Senningen traite de l'échange direct de données à caractère personnel. Les services de police peuvent communiquer des données à caractère personnel provenant de registres spécifiques (voir ci-dessous) directement aux services de police de l'autre partie aux fins prévues à l'article 10 (art. 13, al. 1). Cette disposition couvre également la transmission de données à caractère personnel en l'absence d'une demande à cet effet dans les zones frontalières (art. 13, al. 2). Lorsque des informations sont transmises, l'autorité centrale de la Partie émettrice doit en informer l'autorité centrale du pays destinataire (art. 14).

Anticipant sur le Traité de Prüm évoqué plus haut, le Traité de Senningen offrait également la possibilité de consulter directement les registres d'immatriculation des véhicules (art. 15). En outre, le Traité offre la possibilité d'étendre, à l'avenir, cette consultation directe à d'autres registres contenant des données à caractère personnel (art. 15 al.3).¹⁴

Le Traité de Senningen contient également certaines dispositions sur la manière dont les informations peuvent être échangées. L'article 16 crée la possibilité que l'échange d'informations prenne la forme d'un contact permanent par le biais d'officiers de liaison. Ces officiers de liaison peuvent également accomplir des tâches liées au maintien de l'ordre public et de la sécurité ou de la protection des personnes et des biens (art. 17, al.1).

L'article 24 prévoit la possibilité d'ouvrir des centres de police communs. Ces centres peuvent être compétents pour l'échange et la consultation visés à l'article 13 sur l'ensemble du territoire des Parties contractantes et pas seulement dans les zones frontalières.

Enfin, le Traité de Senningen définit plus précisément certains termes. Par registre, il faut entendre, pour les Pays-Bas, « un registre tel que visé par la loi sur les registres de police » et, pour la Belgique, « la banque de données nationale générale sauf les données soumises à autorisation des autorités judiciaires conformément à la législation nationale. » (Annexe 4).

Au moment de la conclusion du traité, la Belgique et les Pays-Bas n'avaient pas la même compréhension du terme « zone frontalière ». La Belgique a déclaré l'ensemble du territoire national comme étant une zone frontalière, mais les Pays-Bas ont limité cela aux forces de police régionales de l'époque dans les provinces du Limbourg, du Brabant septentrional et de la Zélande (annexe 3).¹⁵

Le Traité d'Enschede

Le deuxième traité bilatéral sur l'échange de données policières qui est pertinent dans le contexte de ce précis est le Traité d'Enschede, auquel l'Allemagne et les Pays-Bas sont parties. Ce traité s'appuie sur la Convention d'application de l'accord de Schengen, mais offre des possibilités plus larges (art. 7).

Elles correspondent dans une large mesure à l'article 27 du Traité de Prüm, mais diffèrent sur les points suivants. L'article 7, alinéa 5, permet l'identification des abonnés au téléphone et des abonnés à d'autres installations de télécommunications, sans restriction quant à l'accès du public. L'article 7, alinéa 2 n'impose aucune restriction d'urgence en ce qui concerne les dénonciations relatives aux armes et aux explosifs ainsi que les dénonciations relatives aux faux et aux escroqueries sur valeurs mobilières. L'article 7 permet en outre l'échange d'informations sur demande concernant les interrogatoires de police (art. 7, al.12), les traces techniques (art. 7, al.13) et la coordination et la mise en œuvre des mesures d'enquête (art. 7, al.14). Ces trois dernières dispositions ne figurent pas dans le traité de Prüm.

L'article 8 du Traité d'Enschede permet aux forces de police et aux procureurs de se contacter directement lorsque des mesures d'enquête urgentes doivent être prises (art. 8). Ce compromis est motivé par le fait qu'aux

¹⁴ À ce jour, la Belgique et les Pays-Bas n'ont pas opté pour cette dernière, mais elle est abordée dans le traité modifié entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à la coopération policière (Trb. 2018, 160), qui a été signé en 2018 mais n'est pas encore en vigueur au moment de la rédaction du présent rapport.

¹⁵ Pour les Pays-Bas, cela a été adapté dans le traité de police Benelux renouvelé 2018 (pas encore en vigueur) aux districts de la région frontalière, la Belgique, en revanche, l'a limité aux arrondissements limitrophes des Pays-Bas ou du Luxembourg.

Pays-Bas, le procureur est chargé de la conduite quotidienne des enquêtes, alors qu'en Allemagne, ce sont les autorités policières qui décident des choix tactiques pendant la conduite des enquêtes.

L'article 15 du Traité d'Enschede concerne la communication spontanée d'informations. « Les autorités des États contractants peuvent, dans des cas exceptionnels et dans le respect du droit national, se communiquer sans demande des informations, y compris des données à caractère personnel, s'il existe des indices que le destinataire a besoin de ces informations pour les enquêtes en matière pénale. Le destinataire est tenu d'évaluer la pertinence des données transmises et de supprimer ou de détruire les données non essentielles ou de les renvoyer à l'autorité qui les a fournies et, si les informations s'avèrent inexactes, d'en informer l'autorité qui les a fournies. ». D'une part, cette disposition offre donc des possibilités plus larges que la décision-cadre suédoise puisqu'elle s'applique également aux infractions non couvertes par le mandat d'arrêt européen. En revanche, l'expression « dans des cas exceptionnels » et la nécessité d'une vérification sont des restrictions par rapport à la décision-cadre susmentionnée.

L'article 20 traite de l'échange spontané d'informations dans le but de maintenir l'ordre public et la sécurité ou de prévenir les infractions pénales. « Conformément droit national, les autorités compétentes des États contractants peuvent, dans des cas individuels, se communiquer mutuellement des informations, y compris des données à caractère personnel, en l'absence de demande à cet effet, lorsqu'il existe des indices que le destinataire a besoin de connaître ces informations pour maintenir l'ordre public et la sécurité ou pour prévenir des infractions pénales. » Elle est également soumise à l'obligation de vérification (art. 15), mais pas à la restriction selon laquelle elle doit concerner des « cas exceptionnels ».

Enfin, l'article 4 est important, car il traite de l'échange (spontané) d'informations qui n'impliquent pas de données à caractère personnel. Pour l'enquête, il est important que les parties « s'informent mutuellement des faits, des liens avec le délinquant et du comportement typique du délinquant sans fournir de données personnelles » (art. 4, al 1a). En outre, ils « échangent mutuellement les informations importantes, à l'exception des données à caractère personnel, afin de planifier les opérations dans le travail quotidien et lors d'événements spéciaux et, à titre de précaution, échangent également mutuellement les informations sur les événements susceptibles d'induire des conséquences sur le territoire de l'autre État contractant » (art. 4, al.1c).

Les demandes concernant les autorités de police sont en principe adressées aux autorités centrales nationales de police (art. 7, al.4). Toutefois, si le centre névralgique de l'infraction et de l'enquête se situe dans les régions frontalières, les demandes peuvent être envoyées et traitées directement entre les autorités de police compétentes (art. 7, al.4 (1)). Cela s'applique également aux cas où « une coopération directe fondée sur des liens entre les actes ou les auteurs dans le cadre d'un cas clairement identifié est effective et a été autorisée par l'autorité centrale de police nationale concernée » (art. 7, al. 4 (2)).

Aux Pays-Bas, on entend par région frontalière les unités de la police nationale dont le territoire est frontalier avec l'Allemagne, ainsi que la mer des Wadden et la mer du Nord (art. 3). En Allemagne, il s'agit du district de la direction de la police d'Osnabrück, dans le Land de Basse-Saxe, ainsi que des districts municipaux (*Kreise*) et des municipalités urbaines (*kreisfreie Städte*) dans les districts administratifs de Düsseldorf, Cologne et Münster, dans le Land de Rhénanie-du-Nord-Westphalie (article 3).

Enfin, il convient de noter qu'afin de faciliter l'échange d'informations entre les autorités policières, des centres communs peuvent également être créés avec l'Allemagne (article 24).

2.3 Les instruments d'échange d'informations fiscales

2.3.1 Dispositions multilatérales et au niveau de l'UE

Modèle de Convention de l'Organisation européenne de coopération économique (OCDE)-2017

Pour l'échange international d'informations fiscales, il est important de commencer par le Modèle de Convention de l'Organisation européenne de coopération économique (OCDE). Ce modèle de convention n'est pas contraignant, mais dans les conventions fiscales, les pays membres adoptent largement ses dispositions. L'article 26 du Modèle de Convention traite de l'échange international de renseignements fiscaux. Cela ne se limite pas aux résidents de l'une des parties, ni aux formes d'imposition sur lesquelles porte principalement le modèle de convention (art. 26, al.1).

Les autorités compétentes peuvent échanger des renseignements pertinents pour la mise en œuvre des dispositions du modèle de convention ou pour la mise en œuvre ou l'application de la législation fiscale nationale, dans la mesure où cela n'est pas contraire au modèle de convention (art. 26, al.1). Ces informations sont soumises aux mêmes obligations de confidentialité que celles prévues par la législation nationale (art. 26, al.2). Les parties ne sont pas tenues de prendre des mesures fiscales administratives dérogeant à la législation et à la pratique administrative de l'État membre émetteur et de l'État membre destinataire (art. 26, al. 3a), de fournir des informations que les autorités de l'État membre destinataire ne peuvent obtenir sur la base de la législation nationale (art. 26, al. 3b), ou de fournir des informations qui doivent rester confidentielles en raison des intérêts des parties privées ou de l'ordre public (art. 26, al. 3c). Lorsque l'État membre requérant demande des informations, l'État membre destinataire est tenu de les obtenir par les moyens dont il dispose, sous réserve des restrictions énoncées au paragraphe 3 (art. 26, al. 4). Ces restrictions ne s'appliquent pas aux informations qui doivent être demandées à des parties privées ou publiques, ou à des particuliers, ou parce qu'elles se rattachent aux droits de propriété d'une personne (art. 26, al.5). L'article 27 traite de la coopération en matière de recouvrement.

La Convention concernant l'assistance administrative mutuelle en matière fiscale (Convention AAMF)

La Convention AAMF a été élaborée par le Conseil de l'Europe et l'OCDE, initialement en 1988 et modifiée en 2010. La convention s'applique à la perception et au recouvrement des impôts et des cotisations de sécurité sociale. Elle joue également un rôle important dans la lutte contre l'évasion et la fraude fiscales, le blanchiment d'argent et la corruption.¹⁶ La Convention AAMF est basée sur les Common Reporting Standards élaborés par l'OCDE. En conséquence, une demande ne peut être refusée au motif que le pays requis n'y a pas d'intérêt propre ou en raison de l'existence d'un secret bancaire. La convention prévoit également des garanties étendues pour protéger la confidentialité des informations échangées.

La Convention AAMF fait une distinction entre l'assistance administrative et l'assistance juridictionnelle en matière pénale (art. 1 al.1). En ce qui concerne l'assistance juridictionnelle en matière de droit pénal fiscal, il est fait référence aux instruments conventionnels relatifs à l'assistance juridictionnelle en matière pénale, tels que décrits ci-dessus. Dans le cadre de l'appréciation de la question de l'opportunité d'engager une procédure pénale, il est permis de demander des informations (art. 4, al. 1).

L'assistance administrative s'étend non seulement à l'échange d'informations, mais aussi à l'assistance au recouvrement et à la délivrance de documents (art. 1, al.1). Les types d'impôts couverts par le traité sont énumérés dans une annexe. Il s'agit, d'une manière générale, des impôts sur le revenu ou les bénéfices, les gains en capital et l'actif net, ainsi que des cotisations obligatoires au titre de la législation sur la sécurité sociale, de la taxe sur les ventes, des droits d'accises, etc. La Convention AAMF, contrairement au Modèle de Convention de l'OCDE, ne prévoit pas d'assistance dans les situations où une évaluation n'a pas encore été faite.

L'article 4 décrit les formes d'assistance. L'obligation d'échanger des renseignements existe si ceux-ci sont vraisemblablement pertinents pour l'établissement et la perception des impôts. Le pays demandeur doit indiquer l'intérêt des informations demandées. Des renseignements peuvent également être échangés spontanément, auquel cas l'intérêt prévisible est déterminé par le pays émetteur.¹⁷ L'échange de renseignements est obligatoire lorsqu'il y a des poursuites par une autorité administrative, ou une procédure devant un tribunal. Les renseignements peuvent être transmis par l'État destinataire à un autre État avec le consentement de l'État émetteur. L'article 6 régit l'échange automatique de renseignements.

La Convention prévoit la possibilité, en cas d'intérêt commun, de mener des contrôles fiscaux simultanés dans deux ou plusieurs pays (article 8). Les pays requis sont libres de décider de coopérer ou non à un tel examen simultané. Les représentants d'un autre État peuvent, sur demande, participer à des contrôles fiscaux à l'étranger (art. 9). Toutefois, l'État où a lieu le contrôle fiscal prend toutes les décisions nécessaires à ce contrôle fiscal.

La possibilité de fournir une assistance au recouvrement est prévue à l'article 11. Les États qui ont accepté cette partie de la Convention AAMF s'engagent à recouvrer une créance fiscale d'un autre État à sa demande, comme s'il s'agissait d'une affaire sur leur propre territoire. Cette assistance peut également être refusée, y compris lorsqu'il s'agit de recouvrer une amende administrative (art. 30). Si la dette n'est pas encore irrévocablement

¹⁶ J. Boonj (2018). Internationale fiscale gegevensuitwisseling. Wolters Kluwer, p. 34.

¹⁷ Boonj, 2018, p. 37.

établie, il est possible de prendre des mesures conservatoires conformément à la législation de l'État requis (art. 12). Toutefois, la loi de l'État requérant s'applique en ce qui concerne tout délai de prescription (art. 14). La même exception s'applique en ce qui concerne les procédures applicables au recouvrement (art. 15).

Une demande d'information doit porter sur des données spécifiques concernant des personnes identifiées : les demandes générales ne sont pas possibles (art. 18). En outre, la règle de l'épuisement s'applique, selon laquelle les informations ne sont demandées que lorsqu'elles ne peuvent être obtenues par les méthodes habituelles applicables au niveau national (article 19). Comme il existe de nombreuses réglementations internationales prévoyant l'échange d'informations, l'article 27 de la Convention AAMF règle la relation avec ces autres réglementations et détermine que la réglementation dont les possibilités de coopération sont les plus larges doit prévaloir.

Cadres pour l'échange de renseignements fiscaux dans le contexte de l'UE

Au sein de l'UE, la coopération administrative en matière fiscale est régie par le Règlement 904/2010 et la Directive 2011/16/UE.¹⁸ La directive a été modifiée à plusieurs reprises afin d'élargir l'échange automatique (obligatoire) d'informations, de mettre en œuvre les CRS, de permettre aux autorités fiscales d'accéder aux procédures de *customer due diligence* réalisées par les institutions financières et de renforcer l'approche de l'évasion fiscale par le biais de structures transfrontalières.¹⁹

Le Règlement 904/2010 prévoit l'échange d'informations à la demande. Cela concerne les autorités compétentes des États membres chargées de la mise en œuvre de la législation sur la TVA (art. 1, al.1). L'article 1 précise la nature de l'information. Les demandes peuvent également porter sur (plusieurs) cas précis (art. 7, al. 1). L'autorité requise fait procéder aux enquêtes administratives nécessaires pour obtenir les informations demandées (art. 7, al. 2). Une enquête administrative spécifique peut également être demandée, sous conditions (art. 7.4). L'article 13 permet l'échange d'informations sans demande préalable. L'échange spontané peut avoir lieu lorsque l'imposition est réputée avoir lieu dans l'État membre de destination et que les informations fournies par l'État membre d'origine sont nécessaires à l'efficacité du système de contrôle de l'État membre de destination (article 13a) ; lorsqu'un État membre a des raisons de croire qu'une infraction à la législation sur la TVA a été commise ou est susceptible d'avoir été commise dans l'autre État membre (article 13b) ; ou lorsqu'il existe un risque de perte de recettes fiscales dans l'autre État membre (article 13c). Le Règlement 904/2010 contient également des exigences procédurales détaillées concernant l'échange d'informations sur demande et l'échange spontané.

La Directive 2011/16/UE s'applique à toutes les taxes perçues par ou pour le compte d'un État membre ou des entités territoriales ou administratives d'un État membre, y compris les autorités locales (art. 2). À l'exception de la taxe sur la valeur ajoutée, à laquelle le règlement 904/2010 fait référence, et des droits de douane et

d'accises. Dans ce cadre, il est possible d'échanger des informations vraisemblablement importantes pour l'administration et l'application de la législation interne des États membres (art. 1). La directive prévoit à nouveau l'échange d'informations sur demande (section I) et l'échange spontané d'informations (section III). L'échange spontané est dans ce cas moins volontaire qu'il n'y paraît, puisque l'article 9, paragraphe 1, prévoit une série de cas dans lesquels l'échange « spontané » d'informations est obligatoire.²⁰ Les possibilités d'échange sont par ailleurs largement similaires à celles du règlement examiné ci-dessus. La section II de la directive prévoit l'échange automatique d'informations sur des catégories spécifiques de revenu et du patrimoine, telles que les revenus professionnels, les jetons de présence et les pensions, en ce qui concerne les résidents de l'autre État membre (article 8).

L'échange d'informations fiscales est soumis à l'obligation du secret professionnel et est protégé par la législation nationale de l'État membre destinataire sur les informations similaires. En principe, elles ne peuvent être utilisées que dans le cadre de la procédure d'établissement et de recouvrement des impôts, y compris les procédures judiciaires et administratives pour infraction à la législation fiscale. Ce n'est que sous certaines

18 Règlement (UE) n° 904/2010 du Conseil du 7 octobre 2010 concernant la coopération administrative et la lutte contre la fraude dans le domaine de la taxe sur la valeur ajoutée (refonte). Journal officiel de l'Union européenne. L268/1 ; Directive 2011/16/UE du Conseil du 15 février 2011 concernant la coopération administrative dans le domaine fiscal et abrogeant la directive 77/799/CEE. Journal officiel de l'Union européenne. L64/1.

19 Voir : Directive (UE) 2015/849 (UE) ; directive (UE) 2015/2376 ; directive (UE) 2016/881 ; directive (UE) 2016/2258 et directive 2018/822.

20 Boonj, 2018, p. 31.

conditions qu'elles peuvent être utilisées à d'autres fins (Règlement, art. 55, al.3 et Directive, art. 16, al.2). Il faut que cela soit autorisé par le droit national et que l'autorité compétente de l'État membre émetteur accorde son autorisation. Cela ne peut être refusé si les informations peuvent être utilisées à des fins similaires dans cet État membre. Les autres restrictions pertinentes sont qu'en vertu de la directive, l'État membre requis n'est pas obligé de procéder à des enquêtes ou de transmettre des informations si sa législation ne lui permet pas de procéder à des enquêtes ou de collecter les informations demandées pour ses propres besoins (art. 17, al. 2). La communication d'informations peut également être refusée lorsqu'elle conduirait à la divulgation de secrets d'affaires ou de secrets analogues, ou d'informations dont la divulgation serait contraire à l'ordre public (art. 17, al. 4). En revanche, le secret bancaire ne peut être invoqué (art. 18, al.2).

La directive 2014/107/UE a introduit des changements importants.²¹ La plupart d'entre eux découlent de l'adoption des Common Reporting Standards (CRS) de l'OCDE dans le cadre de l'échange automatique d'informations sur les comptes financiers. La directive oblige les institutions financières à appliquer les règles d'identification et de déclaration des CRS et les administrations fiscales fournissent ensuite ces données aux autres États membres sur une base automatique, sous réserve des règles en matière de protection de la vie privée.²²

Une modification assez récente de la directive 2018/822/UE²³ implique un nouvel élargissement du cadre réglementaire, notamment afin de lutter plus efficacement contre l'évasion fiscale via des organisations s'étendant sur plusieurs pays. En outre, elle stipule que la transmission d'informations prédéfinies à un autre État membre, sans demande préalable, doit avoir lieu à intervalles réguliers et prédéterminés. Enfin, le principe de disponibilité a été appliqué aux données fiscales. Les « informations disponibles » sont définies comme « des informations figurant dans les dossiers fiscaux de l'État membre qui communique les informations et pouvant être consultées conformément aux procédures de collecte et de traitement des informations applicables dans cet État membre ».

Échange d'informations dans le cadre des douanes et accises

La base juridique de l'assistance mutuelle en matière douanière est définie dans un certain nombre de règlements internationaux. Nous aborderons ici la Convention dite Naples II²⁴ et le code des douanes de l'Union.²⁵

La Convention Naples II permet l'échange d'informations à des fins tant pénales qu'administratives. Elle couvre l'assistance en matière de droits de douane ; de taxes d'effet équivalent, telles que les droits antidumping et les taxes compensatoires ; de législation dans le domaine de la sécurité, de la santé, de l'économie et de l'environnement et de droits d'accises.²⁶ On entend par « réglementation douanière nationale » l'ensemble des dispositions législatives, réglementaires et administratives dans le cadre desquelles l'administration douanière est totalement ou partiellement compétente pour les mouvements transfrontaliers de marchandises faisant l'objet d'interdictions, de restrictions ou de contrôles, ou de droits d'accises non harmonisés.

La convention prévoit la possibilité de prévenir et de détecter les infractions aux dispositions douanières nationales et de poursuivre et de sanctionner les infractions aux dispositions douanières communautaires et nationales. Ce n'est que dans ce contexte que l'échange de données à caractère personnel est possible, c'est-à-dire « toute information concernant une personne physique identifiée ou identifiable » (art. 4, al. 8).

21 Directive 2014/107/UE du Conseil du 9 décembre 2014 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique d'informations dans le domaine fiscal. Journal officiel de l'Union européenne, L359/1.

22 Booi, 2018, p. 28.

23 Directive (UE) 2018/822 du Conseil du 25 mai 2018 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique d'informations dans le domaine de la fiscalité des structures transfrontalières soumises à notification. Journal officiel de l'Union européenne L139/1.

24 Acte du Conseil du 18 décembre 1997 établissant la convention fondée sur l'article K.3 du traité sur l'Union européenne, relative à l'assistance mutuelle et à la coopération entre les administrations douanières. Journal officiel des Communautés européennes C24/1.

25 Les règlements suivants concernent les dispositions douanières communautaires et ne sont donc pas repris dans le cadre de l'Euregio Meuse-Rhin. Règlement (CE) n° 515/97 du Conseil du 13 mars 1997 relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole. Journal officiel des Communautés européennes L82/1 ; Règlement (UE) n° 389/2012 du Conseil du 2 mai 2012 concernant la coopération administrative dans le domaine des droits d'accises et abrogeant le règlement (CE) n° 2073/2004. Journal officiel de l'Union européenne L121/1. Modifié le 1-7-2013.

26 Booi, 2018, p. 59.

Sur la base de la convention Naples II, des informations peuvent être échangées sur demande afin de lui permettre de prévenir, rechercher et réprimer les infractions (art. 10, al. 1). Les agents habilités sur le territoire étranger peuvent, sous réserve d'instructions détaillées de l'autorité requise, recueillir les informations visées au paragraphe 1 et prendre copie de documents dans les bureaux de l'État membre requis (art. 10, al. 3). Les informations ne peuvent être utilisées que dans le but d'assurer l'évaluation correcte des droits et taxes à l'importation ou à l'exportation ou en rapport avec des faits qui permettent de soupçonner qu'une infraction liée à la législation douanière, y compris la législation concernant la sécurité, la santé, les questions économiques et environnementales, a été commise ou est sur le point de l'être.²⁷ L'article 17 permet l'échange spontané de renseignements sur les infractions projetées ou commises, notamment des renseignements sur les marchandises concernées et sur les nouveaux moyens et méthodes employées pour commettre ces faits.

Les informations échangées sont soumises à des mesures de protection des données. En principe, la convention permet de transmettre des informations à d'autres autorités, mais cela nécessite le consentement de l'État membre qui a fourni les informations (art. 25, al.2, a). La convention permet aux parties de refuser l'assistance lorsque celle-ci pourrait porter atteinte à l'ordre public ou à d'autres intérêts essentiels de l'État membre concerné, ou lorsque l'action demandée serait disproportionnée par rapport à la gravité de l'infraction présumée (art. 28).

Enfin, le code des douanes de l'Union comprend une section (section 1) sur l'échange d'informations.²⁸ Cette section traite de l'échange d'informations entre les autorités douanières et entre les opérateurs économiques et les autorités douanières. Les dispositions portent sur l'enregistrement des opérateurs économiques, les moyens d'échange et de stockage des informations, la délégation de pouvoirs, la protection des données et l'utilisation des systèmes électroniques.

2.3.2 Dispositions bilatérales

Coopération fiscale entre les Pays-Bas et la Belgique

Les Pays-Bas et la Belgique ont conclu une convention fiscale bilatérale en 2001.²⁹ La convention s'applique aux impôts sur le revenu et sur la fortune (art. 2, al.1). L'article 29 règle l'échange d'informations entre les Pays-Bas et la Belgique. La convention permet l'échange de renseignements vraisemblablement pertinents pour appliquer les dispositions de la convention ou celles de la législation interne des États contractants relative aux impôts visés par la convention dans la mesure où l'imposition que cette législation interne prévoit n'est pas contraire à la convention (art. 29, al 1). L'échange de renseignements n'est pas restreint par les articles 1 (champ d'application *ratione personae*) et 2 (champ d'application *ratione materiae*) de la convention. La convention prévoit la possibilité d'utiliser les renseignements à d'autres fins si, en vertu de la législation des deux États, elles peuvent être utilisées à ces autres fins et si l'autorité compétente de l'État qui les a fournies consent à cette utilisation (art. 29, al. 2).

L'accord n'impose aucune obligation de prendre des mesures administratives qui s'écartent de la législation interne, de transmettre des détails qui ne sont pas disponibles en vertu de la législation et de la pratique administrative courante de cet État ou de l'autre État contractant ; ni de transmettre des renseignements qui révéleraient un secret commercial, industriel, professionnel ou un procédé commercial ou des renseignements dont la divulgation serait contraire à l'ordre public (art. 29, al.3).

Depuis le 1er janvier 2016, les CRS sont entrés en vigueur en Belgique et aux Pays-Bas. Cela implique que les données sont depuis lors échangées automatiquement entre les pays. Cependant, l'échange sur cette base ne concerne pas les données antérieures à 2016. L'échange automatique de données s'opère entre la Belgique et les Pays-Bas depuis des années. En 2009, la Belgique et les Pays-Bas avaient déjà convenu que la première n'invoquerait plus le secret bancaire, ce qui a rendu possible l'échange automatique à partir du 1er janvier 2010, et l'échange de données bancaires sur demande avec effet rétroactif au 1er janvier 2008.

Coopération fiscale entre les Pays-Bas et l'Allemagne

L'Allemagne et les Pays-Bas ont conclu une convention fiscale bilatérale en 2012. Cette convention est

²⁷ Booiij, 2018, p. 65.

²⁸ Règlement (UE) n° 952/2013 du Parlement européen et du Conseil du 9 octobre 2013 établissant le code des douanes de l'Union (refonte). Journal officiel de l'Union européenne. L269/1.

²⁹ Convention entre le Royaume des Pays-Bas et le Royaume de Belgique tendant à éviter les doubles impositions et à prévenir l'évasion fiscale en matière d'impôts sur le revenu et sur la fortune, avec protocoles ; Luxembourg, 5 juin 2001, Série des traités 2001, n° 136.

comparable au traité belgo-néerlandais en ce qui concerne l'échange d'informations. La convention permet aux services fiscaux des Pays-Bas et d'Allemagne d'échanger des renseignements vraisemblablement pertinents pour appliquer les dispositions de la convention ou celles de la législation interne des États contractants relative aux impôts visés par la convention dans la mesure où l'imposition que cette législation interne prévoit n'est pas contraire à la Convention (art. 29, al. 1). L'échange de renseignements n'est pas restreint par les articles 1 (champ d'application *ratione personae*) et 2 (champ d'application *ratione materiae*) de la convention. La convention prévoit également la possibilité d'utiliser les renseignements à d'autres fins si, en vertu de la législation des deux États, elles peuvent être utilisées à ces autres fins et si l'autorité compétente de l'État qui les a fournies consent à cette utilisation (art. 27, al. 2).

En outre, comme l'accord belgo-néerlandais, cet accord s'applique aux renseignements à partir de 2016, pour cause d'adoption des CRS. Les données qui peuvent être échangées automatiquement et la manière de le faire sont définies en 1997 dans le *Regeling tussen Nederland en Duitsland inzake de uitwisseling van inlichtingen op het gebied van de belastingen*.³⁰ Certaines informations sont échangées automatiquement (art. 1) et d'autres spontanément (art. 2).

En outre, depuis 2009, une déclaration d'intention commune existe entre les Pays-Bas et l'Allemagne dans le domaine de l'échange de renseignements sur la TVA. En octobre 2021, une déclaration d'intention commune est entrée en vigueur entre le ministère fédéral des Finances de la République fédérale d'Allemagne et le ministère des Finances des Pays-Bas sur l'échange transfrontalier de renseignements dans le domaine de la fiscalité directe. Cela permet aux collaborateurs mandatés (personnes de contact) chargés des impôts directs dans les bureaux désignés pour cette tâche de l'administration fiscale et douanière néerlandaise dans la région frontalière avec l'Allemagne d'échanger directement des renseignements avec les collaborateurs mandatés (personnes de contact) chargés des impôts directs dans les bureaux de l'administration fiscale et douanière des États allemands de Rhénanie-du-Nord-Westphalie et de Basse-Saxe dans la région frontalière avec les Pays-Bas. Cela peut impliquer l'échange de renseignements sur demande ou la transmission spontanée de renseignements. Les collaborateurs mandatés peuvent également se rendre physiquement dans les autres bureaux fiscaux visés par la déclaration d'intention. Ces bureaux fiscaux, tant aux Pays-Bas qu'en Allemagne, sont mentionnés dans la déclaration d'intention.³¹

Enfin, les Pays-Bas ont conclu avec l'Allemagne une convention bilatérale sur l'assistance au recouvrement des dettes fiscales et la délivrance de documents.³² En ce qui concerne l'échange de renseignements, cette convention est comparable à celle décrite ci-dessus et à celle conclue avec la Belgique (art. 12). La possibilité existe ici aussi de transmettre les renseignements échangés à des tiers, aux mêmes conditions (art. 13).

Coopération fiscale entre la Belgique et l'Allemagne

La Belgique et l'Allemagne ont également conclu une convention fiscale bilatérale.³³ Dans le domaine de l'échange d'informations, cette convention est identique à la convention fiscale belgo-néerlandaise (art. 26). Les informations obtenues ne peuvent être divulguées à des tiers. Les renseignements obtenus ne peuvent être communiqués, à l'exception du contribuable ou de son mandataire, qu'aux personnes ou autorités chargées

de l'établissement ou du recouvrement des impôts visés par la convention et des contestations et recours y afférents, ainsi qu'aux autorités judiciaires aux fins de poursuites pénales (art. 26, al.1).

Coopération douanière dans le Benelux

Au niveau du Benelux, la convention dite de coopération douanière du Benelux est importante.³⁴ Les dispositions qu'elle contient à propos de l'échange d'informations sont comparables à celles de la Convention Naples II concernant l'échange sur demande et spontané. La Convention concerne l'application des dispositions légales des trois pays, en lien avec la réalisation des objectifs de l'Union économique Benelux, tels que déterminés par le Comité des Ministres (Art. 2).

³⁰ Règlement du 16 octobre 1997, n° AFZ97/3934, Journal officiel 1997, 235.

³¹ Décision du Secrétaire d'État aux finances du 15 octobre 2021, Journal officiel néerlandais 2021, 45227, V-N 2021/48.10.

³² Traité entre le Royaume des Pays-Bas et la République fédérale d'Allemagne concernant l'assistance administrative mutuelle pour le recouvrement des créances fiscales et la délivrance de documents, Série des traités 1999, n° 113.

³³ Convention entre le Royaume de Belgique et la République fédérale d'Allemagne tendant à éviter les doubles impositions et à régler certaines autres questions en matière d'impôts sur le revenu et sur la fortune, y compris les impôts commerciaux et fonciers.

³⁴ Convention relative à la coopération administrative et pénale dans le cadre de la réglementation concernant la réalisation des objectifs de l'Union économique Benelux (29-04-1969).

En ce qui concerne la collecte d'informations sur le territoire d'un des autres États membres, le traité Benelux offre des possibilités plus larges. Les fonctionnaires, dûment autorisés par les autorités compétentes de leur pays, peuvent, avec l'accord des autorités compétentes du pays requis et dans les mêmes conditions que les fonctionnaires de ce pays : recueillir des informations auprès des bureaux de l'administration de ce pays dans la mesure où elles se rapportent à l'article 2 ; effectuer des enquêtes et des contrôles conjoints avec les fonctionnaires du pays requis et coopérer avec eux sous leur direction (art. 6).

Les données obtenues peuvent être divulguées à d'autres personnes à d'autres fins, si l'autorité qui a communiqué les données y a expressément consenti dans le respect de la loi de son pays et à condition que la loi du pays de l'autorité qui a reçu les données ne l'interdise pas (art. 6.4).

2.4 Les instruments d'échange d'informations sur la répression administrative

Il n'existe pas de cadre juridique complet pour l'échange international de renseignements sur la répression administrative. Ce cadre n'a été créé que dans certains cas de fraude sociale. Cela ne signifie pas qu'il n'existe pas de possibilités d'échange de renseignements sur la répression administrative, mais ceux-ci sont encadrés par le règlement général sur la protection des données. En outre, on peut se référer à la Convention européenne du 15 mars 1978, adoptée par le Conseil de l'Europe, relative à l'obtention de renseignements et de preuves à l'étranger en matière administrative. Cette convention a été signée et ratifiée par la Belgique et l'Allemagne, mais pas par les Pays-Bas.³⁵ Pour cette raison, elle n'est pas examinée plus avant ici. En outre, nous abordons brièvement les réglementations relatives au travail et à la sécurité sociale.

2.4.1 Cadres au niveau de l'UE

Le règlement général sur la protection des données

Le règlement général sur la protection des données (RGPD), entré en vigueur en 2018, porte sur la réglementation relative à la protection des personnes physiques dans le cadre du traitement et de la libre circulation des données à caractère personnel.³⁶ En tant que tel, le RGPD est pertinent à la fois pour l'échange transfrontalier de renseignements entre les autorités répressives administratives, dans la mesure où aucun autre cadre juridique pertinent ne s'applique, et pour l'échange de renseignements à l'intérieur d'un pays (voir chapitre 4).

Les dispositions les plus importantes pour le traitement des données personnelles par les organes administratifs sont les articles 5 et 6 du RGPD. Ces dispositions stipulent, entre autres, que le traitement des données à caractère personnel doit être licite, loyal et transparent (art. 5, al. 1er, a). En outre, le traitement des données à caractère personnel est lié à la finalité, comme l'indique l'article 5, paragraphe 1, point b : « les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités ». L'article 5 énonce les conditions que le traitement des données à caractère personnel doit remplir pour être licite. Les conditions de l'article 5 s'appliquent de manière cumulative. Les principes généraux du traitement des données sont : la licéité, la loyauté et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité et la responsabilité. Ils sont décrits à l'article 5 du RGPD et développés dans d'autres articles du RGPD. La condition la plus importante pour le traitement des données à caractère personnel par les autorités (répressives) administratives est que le traitement doit être nécessaire au respect d'une obligation légale incombant au responsable du traitement.

L'article 6, paragraphe 1, contient les motifs du traitement des données. Il doit toujours y avoir au moins un fondement présent. Ces motifs sont les suivants : consentement; nécessaire à l'exécution d'un contrat; nécessaire au respect d'une obligation légale; nécessaire à la sauvegarde des intérêts vitaux de la personne

35 Van Daele et Bollens voient cependant des possibilités d'invoquer cette convention. Voir : D. van Daele & S. Bollens (2019). De informatie-uitwisseling met het oog op de bestuurlijke aanpak van mensenhandel: een rechtsvergelijkend onderzoek in België en Nederland. KU Leuven.

36 Règlement (UE) 2016/79 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Journal officiel de l'Union européenne, L119/1.

concernée ou d'une autre personne physique; nécessaire à l'accomplissement d'une mission d'intérêt général; nécessaire aux fins des intérêts légitimes du responsable du traitement ou d'un tiers.

La notion de données à caractère personnel recouvre toute information relative à une personne physique identifiée ou identifiable, quels que soient sa nature, son contenu ou sa forme (art. 4, al. 1). Cela comprend des informations tant objectives que subjectives. Le support de l'information n'est pas pertinent. Une personne physique est identifiable si son identité peut être établie directement ou indirectement. Il s'agit notamment d'un élément identifiable, tel qu'un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou d'un ou plusieurs éléments caractéristiques de son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (art. 4, al. 1). En outre, le RDPD s'étend aux situations dans lesquelles des tiers, autres que le responsable du traitement, sont en mesure de déterminer, par tout moyen raisonnable, à quelle personne ces informations se rapportent. En cas de pseudonymisation, les informations concernant une personne physique ne sont plus considérées comme des données à caractère personnel si cette pseudonymisation est absolue et ne peut être éliminée par aucun moyen raisonnablement susceptible d'être utilisé.³⁷ Le RGPD ne s'applique pas aux informations relatives aux personnes morales. Les informations doivent toujours être considérées comme des données à caractère personnel si les données relatives aux personnes morales contiennent également des informations sur des personnes physiques identifiées ou identifiables.³⁸

Le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement de données à caractère personnel contenues ou appelées à être contenues dans un fichier (art. 2, al. 1). Dans le cadre du RGPD, un fichier est tout ensemble structuré de données à caractère personnel accessibles selon certains critères (art. 4, al. 6). Le concept de traitement des données personnelles est interprété de manière large dans le RGPD. Il s'ensuit que le traitement d'informations dans le cadre de l'approche administrative de la criminalité n'est possible que dans les limites du RGPD.

Traitement licite

Les données personnelles doivent être traitées de manière licite, loyale et transparente (art. 5, al. 1, a RGPD). Les données personnelles doivent être traitées conformément aux règles applicables. Le traitement doit également être vérifiable à chaque étape de la procédure. La forme de conservation doit garantir que la personne physique concernée ne puisse être identifiée plus longtemps que nécessaire aux finalités pour lesquelles les données personnelles sont traitées (art. 5 al. 1, e RGPD). Le RGPD autorise le traitement des données lorsque la personne concernée a donné son consentement explicite ; lors de l'exécution d'un contrat auquel la personne concernée est partie ; lorsque le responsable du traitement est tenu de respecter une obligation légale ; lorsque les intérêts vitaux de la personne concernée ou d'une autre personne physique sont en jeu ; ou pour l'exécution d'une mission d'intérêt public ou dans l'exercice de l'autorité publique dont est investi le responsable du traitement (art. 6, al.1). Ce dernier point est particulièrement pertinent en ce qui concerne l'échange d'informations administratives par-delà les frontières nationales. On peut supposer qu'il est dans l'intérêt d'une autorité chargée de l'application de la loi de soutenir la lutte (éventuelle) contre les activités criminelles d'une autre autorité locale grâce à l'échange d'informations détenues par cette autorité. ³⁹

Le principe de finalité

Le principe de finalité exige que les données à caractère personnel ne soient collectées que pour des finalités déterminées, explicites et légitimes (art. 5, al. 1, b). Le traitement de données à caractère personnel sans finalité déterminée ou pour une finalité implicite est exclu. Le traitement réalisé à toutes fins utiles doit être considéré comme illégal.

Les données à caractère personnel ne peuvent être traitées que d'une manière compatible avec les finalités déclarées (art. 5, al. 1, (b)). Aucune base juridique distincte n'est requise pour cela. La base juridique de la collecte initiale des données personnelles concernées est suffisante. Sur la base du droit de l'Union ou du droit national, les États membres peuvent préciser les tâches et les finalités pour lesquelles un traitement ultérieur des données à caractère personnel doit être considéré comme licite et compatible avec les finalités initiales. ⁴⁰

³⁷ Considérant 26 du préambule du RGPD.

³⁸ Considérant 14 du préambule du RGPD.

³⁹ J. Theunis, D. Bijmens & G. Huts (2020). Les possibilités et impossibilités d'échange d'informations entre administrations locales dans le cadre de l'approche administrative du crime organisé. Université de Hasselt.

⁴⁰ Considérant 50 du préambule du RGPD.

Les données à caractère personnel obtenues pour une finalité déterminée précis peuvent, sous certaines conditions, être traitées ultérieurement pour une autre finalité. L'exigence est que les objectifs ne soient pas incompatibles ; il n'est pas exigé que les finalités soient identiques. Lors de l'évaluation de la compatibilité des finalités, tous les facteurs pertinents doivent être pris en compte, tels que les dispositions légales et réglementaires applicables et les attentes raisonnables de la personne concernée. La nature des données, les risques potentiels pour la vie privée et l'intérêt du responsable du traitement - défini à l'art. 4, al. 7 RGPD - peuvent également être considérés comme des facteurs pertinents.

Le responsable du traitement agit sur la base d'un intérêt légitime si, en réponse à une infraction ou à une menace pour la sécurité publique, il transmet des données à caractère personnel à une autorité compétente. Cela s'applique tant aux cas individuels qu'à plusieurs cas connexes concernant la même infraction pénale ou la même menace pour la sécurité publique. La transmission des données à caractère personnel et/ou leur traitement ultérieur par l'autorité destinataire devraient être interdits si le traitement des données à caractère personnel est incompatible avec une obligation de confidentialité légale, professionnelle ou tout autre obligation contraignante de confidentialité.⁴¹

Les autorités publiques qui reçoivent des données à caractère personnel dans le cadre d'une enquête particulière menée conformément au droit de l'Union ou au droit national ne sont pas considérées comme des destinataires (art. 4, al. 9). Cette règle concerne les autorités publiques auxquelles les données à caractère personnel sont divulguées sur la base d'une obligation légale afin d'accomplir leur mission publique. Les données personnelles peuvent également être communiquées, entre autres, à des autorités administratives indépendantes. Une demande de communication de données à caractère personnel par ces autorités doit être faite par écrit et doit être motivée. Il doit s'agir d'une demande occasionnelle, qui ne peut pas concerner un fichier entier et ne doit pas aboutir à l'interconnexion de dossiers. Le traitement des données personnelles reçues doit toujours respecter les règles de protection applicables aux finalités du traitement.⁴²

En bref, il doit y avoir un lien clair entre la finalité initiale pour laquelle les informations ont été collectées et celle du traitement ultérieur. En outre, il est important de savoir si la personne concernée peut raisonnablement s'attendre à une utilisation ultérieure des données ; le nouveau traitement était-il prévisible à la lumière de la collecte initiale des informations ? Enfin, le cadre dans lequel traitement prend place est pertinent : les garanties d'accompagnement, la nature des données à caractère personnel et les conséquences possibles du traitement ultérieur peuvent jouer un rôle dans cette évaluation.⁴³

Le principe de proportionnalité

Le traitement des données à caractère personnel doit être adapté aux finalités envisagées, mais il doit en même temps être limité à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées (art. 5, al. 1, (c)). Ce faisant, il convient toujours d'examiner quelles données à caractère personnel sont pertinentes aux fins du traitement envisagé.

Les aspects pertinents qui jouent un rôle dans cette considération sont les suivants : les informations fournies sont-elles adéquates sans être excessives ; les informations partagées sont-elles limitées à ce qui est strictement nécessaire à la finalité pour laquelle elles sont traitées (« traitement minimal des données »). Si nécessaire, les informations peuvent être limitées ou rendues anonymes afin de ne transmettre seulement les données strictement nécessaires.⁴⁴

Législation européenne en matière de travail et de sécurité sociale

Dans le contexte de la libre circulation des travailleurs, nous examinons brièvement ci-dessous la directive dite d'exécution 2014/67/UE, qui a été adoptée en 2014.⁴⁵ La directive sous-jacente 96/71/CE vise à protéger les travailleurs qui peuvent être vulnérables en raison de leur situation (travail temporaire dans un pays

⁴¹ Considérant 50 du préambule du RGPD.

⁴² Considérant 31 du préambule du RGPD.

⁴³ Theunis, Bijmens & Huts, 2020.

⁴⁴ Theunis, Bijmens & Huts, 2020.

⁴⁵ Directive 2014/67/UE du Parlement européen et du Conseil du 15 mai 2014 relative à l'exécution de la directive 96/71/CE concernant le détachement de travailleurs effectué dans le cadre d'une prestation de services et modifiant le règlement (UE) n° 1024/2012 concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur (« le règlement IMI »). Journal officiel de l'Union européenne. L159/11.

étranger, difficultés à trouver une assistance juridique ou une autre représentation adéquate, connaissance insuffisante des lois, des autorités et de la langue locales). La directive s'applique aux entreprises qui détachent temporairement des travailleurs dans un État membre autre que celui dont la législation régit la relation de travail. L'objectif de la directive de répression est de prévenir les abus et le contournement des règles applicables en matière de détachement et d'améliorer la surveillance.

La directive de répression contient des dispositions relatives à une bonne coopération administrative et à l'assistance mutuelle (art. 6). Elle fournit également une base juridique pour l'utilisation du système d'information sur le marché intérieur (IMI) pour l'échange d'informations afin de faciliter la coopération administrative (art. 18). L'article 6 permet aux États membres de formuler des demandes d'information motivées et de procéder à des vérifications, inspections et enquêtes auprès des autorités compétentes en ce qui concerne les conditions de détachement énumérées à l'article 1er, alinéa 3 de la directive 96/71/CE (art. 6, al. 2). Ceci est soumis à la restriction que les informations échangées ne soient utilisées que dans le cadre de la ou des finalités pour lesquelles elles ont été demandées (art. 6, al. 8).

Dans le domaine de la sécurité sociale, deux règlements sont pertinents : les règlements (CE) 883/2004 et 987/2009 concernant respectivement la coordination des systèmes de sécurité sociale et leur mise en œuvre.⁴⁶ L'échange de données est possible et se déroule conformément aux règles communautaires relatives à la protection des personnes physiques à l'égard du traitement et de la libre circulation des données à caractère personnel. Le règlement 987/2009 prévoit que les institutions compétentes fournissent ou échangent sans délai toutes les données nécessaires pour établir les droits et obligations des personnes auxquelles le règlement 883/2004 s'applique. Ces données peuvent être échangées entre les États membres directement par les institutions elles-mêmes ou indirectement par l'intermédiaire des organismes de liaison (art. 2, al. 2). L'échange électronique d'informations est considéré comme le moyen approprié de le faire.

2.4.2 Cadres juridiques bilatéraux

Dans le domaine de la législation sur la sécurité sociale, les Pays-Bas et la Belgique ont conclu un accord bilatéral prévoyant une assistance administrative mutuelle.⁴⁷ Les données doivent être nécessaires au bon accomplissement de la mission d'une institution compétente (art. 7, al. 2). Les données ne peuvent être utilisées que pour l'application des législations respectives des Parties contractantes, notamment pour les règles concernant la détermination de la législation applicable et pour les règles concernant la vérification, dans la mesure nécessaire, du droit des personnes concernées aux prestations telles que définies à l'article 3 de la présente Convention (art. 8, al. 3). En outre, il peut être fait référence à l'accord sur l'échange de données électroniques visant à améliorer l'application de la législation en matière de sécurité sociale en Belgique et aux Pays-Bas, qui a été signé le 9 avril 2018. Cet accord stipule également que les données échangées ne peuvent être utilisées qu'aux finalités de l'application de la législation sur la sécurité sociale (art. 6). Par conséquent, il n'existe aucune possibilité de fournir les informations obtenues de l'étranger à d'autres autorités répressives administratives.⁴⁸

Les Pays-Bas et l'Allemagne ont également conclu un accord bilatéral dans le cadre de la fraude aux prestations de sécurité sociale.⁴⁹ La convention concerne les autorités chargées de lutter contre la fraude aux prestations et cotisations de sécurité sociale par le travail et aux prestations de base pour les demandeurs d'emploi, ainsi que le travail non déclaré et le travail temporaire transfrontalier illégal (art. 1, al.1). La Convention permet de fournir les informations nécessaires à la bonne exécution des tâches de ces organes, y compris les données à caractère personnel, sur demande par le biais de l'assistance mutuelle et de la transmission de documents (art. 5, al. 4). Ces informations peuvent également être fournies spontanément (art. 5, al. 5). Les demandes

⁴⁶ Règlement (CE) n° 883/2004 du Parlement européen et du Conseil du 29 avril 2004 portant sur la coordination des systèmes de sécurité sociale. Journal officiel de l'Union européenne. L166/1 ; Règlement (CE) n° 987/2009 du Parlement européen et du Conseil du 16 septembre 2009 modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale.

⁴⁷ Traité entre le Royaume des Pays-Bas et le Royaume de Belgique pour le développement de la coopération d'assistance administrative mutuelle dans le domaine de la sécurité sociale, 6 décembre 2010. Trb. 2013, n° 79.

⁴⁸ Van Daele & Bollens, 2019.

⁴⁹ Convention entre le Royaume des Pays-Bas et la République fédérale d'Allemagne relative à la coopération en matière de lutte contre la fraude transfrontalière aux prestations et cotisations de sécurité sociale du travail et aux prestations de base des demandeurs d'emploi, ainsi qu'au travail non déclaré et au travail temporaire transfrontalier illégal (Convention germano-néerlandaise pour la lutte contre le travail au noir transfrontalier) (Série des *traités* 2012, n° 45).

ou les informations spontanées doivent contenir des détails sur les entreprises ou les personnes concernées, ainsi qu'une description brève et claire des faits. Les demandes doivent également préciser l'autorité requérante, l'objet et le motif de la demande ainsi que les informations ou les traitements demandés (art. 6). Il est intéressant de noter que la Convention prévoit certaines possibilités d'utilisation des informations à des finalités autres que celles pour lesquelles elles ont été transmises. L'utilisation est également autorisée pour la prévention et la poursuite d'infractions pénales graves, ainsi que pour prévenir des menaces importantes à la sécurité publique (art. 8, al. 2).

2.5 Échange direct de renseignements en diagonale

L'attention accrue accordée à l'approche administrative a entraîné un échange plus fréquent d'informations entre les autorités répressives administratives et les instances d'enquête criminelle.⁵⁰ Aux Pays-Bas, on parle désormais d'une « approche intégrale », dans laquelle les autorités fiscales sont également impliquées. Les possibilités d'échange d'informations seront abordées au chapitre 4 de ce précis. Nous nous limiterons ici brièvement aux possibilités d'échange transfrontalier direct d'informations entre des autorités ayant des tâches et des responsabilités différentes, que nous appellerons ici la coopération « diagonale ».

La question est de savoir si les autorités pénales, administratives et fiscales d'un pays peuvent échanger des informations avec l'une des autres autorités du même type à l'étranger. Les cadres internationaux examinés ci-dessus offrent peu ou pas de possibilités explicites pour un tel échange. Il a été décrit plus haut que le traité d'Enschede permet un échange direct entre le ministère public néerlandais et la police allemande, mais cet arrangement doit être considéré avant tout comme fonctionnel et relatif aux différences de compétences, et non comme visant spécifiquement l'échange de renseignements en tant que tel.

Seul le Traité Benelux révisé sur la coopération policière, qui n'est pas encore entré en vigueur, crée la possibilité pour les services compétents de se transmettre mutuellement, dans la mesure où cela n'est pas explicitement interdit par le droit national de la Partie contractante requise, des données à caractère personnel et des informations sur demande pour l'exécution de leurs tâches légales afin que des mesures administratives soient prises par les autorités publiques compétentes à cette fin en vue de prévenir les infractions pénales et de maintenir l'ordre et la sécurité publics.⁵¹

Les autorités fiscales ne peuvent pas échanger directement des informations avec les instances d'enquête criminelle, ni avec les autorités répressives administratives, sauf dans le cadre d'enquêtes fiscales criminelles.

⁵⁰ T. Spapens, M. Peters & D. Vandaele (2015). Administrative measures to prevent and tackle crime. Eleven International Publishing.

⁵¹ Traité entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas relatif à la coopération policière. Bruxelles, le 23 juillet 2018. Série des traités 2018, n° 160.

3 Les cadres juridiques nationaux

3.1 Introduction

Ce chapitre se concentre sur la question de savoir comment la Belgique, l'Allemagne et les Pays-Bas ont mis en œuvre les cadres internationaux pour l'échange d'informations, tels que décrits dans le chapitre précédent, dans la législation nationale. Là encore, il s'agit des cadres d'échange d'informations en matière de droit pénal, d'informations fiscales et d'informations administratives. La mise en œuvre dans la législation nationale des cadres internationaux sur la sécurité sociale et le droit du travail est omise dans le but d'alléger ce manuel. Nous aborderons successivement la Belgique (section 3.2), l'Allemagne (section 3.3) et les Pays-Bas (section 3.4).

3.2 Les cadres juridiques nationaux en Belgique

3.2.1 Échange international d'informations en matière pénale

L'entraide judiciaire est réglementée en Belgique par la loi sur la transmission policière internationale de données à caractère personnel et d'informations à finalité judiciaire, l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du Code d'instruction criminelle (EJI). Cette loi comporte un règlement distinct pour le transfert des données de police et les demandes d'entraide judiciaire internationale.

L'échange de données de police

Point de contact opérationnel unique

La police intégrée belge est structurée en deux niveaux, à savoir la police locale et la police fédérale. La police fédérale est placée sous l'autorité du ministre de l'Intérieur et du ministre de la Justice et, avec l'administration des douanes et accises, elle a été désignée par la Belgique comme une instance répressive habilitée à fournir des informations, comme le prévoit l'article 2, point a), de la Décision-cadre suédoise.⁵² La Direction de la coopération policière internationale de la police fédérale (CGI) est responsable de la coopération policière internationale. Le CGI fonctionne directement sous le Commissariat général et est donc sous l'autorité directe du Commissaire général. Au sein du CGI, le point de contact opérationnel unique (SPOC) s'occupe principalement de l'échange international d'informations policières et de l'émission et du traitement des alertes internationales. Le SPOC enregistre et traite tous les messages opérationnels, y compris ceux provenant d'Interpol, d'Europol, des officiers de liaison et des forces de police. En outre, il traite les messages entrants et sortants des Centres de coopération policière et douanière (CCPD) de Tournai (BE-FR), Kerkrade (BE-NL-DE) et Luxembourg (BE-LUX-FR-DE).⁵³ Les différents canaux d'échange d'informations internationales sont ainsi intégrés au sein du SPOC. Le SPOC relève du National Incident Point (NIP), un service permanent 24h/24 et 7j/7 composé du CGI, de la direction centrale des opérations de police judiciaire (DCOPJ) et de la direction des opérations et de la fonction de police administrative (DOFPA).

Loi de 2004 sur l'entraide judiciaire internationale

Avec la loi modificative du 15 mai 2014, la loi initiale de 2004 a été complétée par un nouveau chapitre intitulé : « La transmission policière internationale des données à caractère personnel et d'informations à finalité judiciaire ». ⁵⁴ Ce chapitre concerne la transposition de la Décision-cadre suédoise en droit belge et crée ainsi une base juridique en droit belge pour le transfert de données policières vers d'autres États membres de l'UE. ⁵⁵

L'ensemble du dispositif se trouve à l'article 2 de la loi EJI, qui se compose de sept sections. Comme on peut partiellement le déduire du titre de la section, il s'agit de la transmission de données à caractère personnel et

⁵² Politie.be, Federale Politie, consulté le 07 octobre 2021 ; Déclaration du Royaume de Belgique concernant la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, Bruxelles, 5 septembre 2008 (10.09) (OR fr) 12645/08, p. 2.

⁵³ La gestion de l'information, le cœur de notre métier, Rapport annuel 2017 de la police fédérale.

⁵⁴ Loi du 15 mai 2014 modifiant la loi du 9 décembre 2004 sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du code de procédure pénale, *M.B.*, 7 août 2014.

⁵⁵ Voir l'article 2/1 de la loi sur l'aide juridique ; le règlement s'applique également aux pays associés de l'espace Schengen, mais compte tenu du champ d'application du présent précis, il n'y sera pas fait référence.

d'informations à finalité judiciaire qui sont directement disponibles ou directement accessibles aux services de police belges (art. 2/2 EJI). L'exigence de finalité judiciaire implique que l'objet de la transmission doit être conforme aux tâches de police judiciaire telles que décrites à l'article 15 de la loi sur la fonction de police.⁵⁶ L'exigence de disponibilité ou d'accessibilité directe implique que les services de police disposent déjà eux-mêmes des données ou qu'ils aient légalement accès aux données dont d'autres autorités, services publics ou privés ou personnes disposent (art. 2/2 EJI). Il s'agit par exemple des données et informations contenues dans la Banque de données Nationale Générale (sauf si un marquage indique qu'elles sont soumises à des restrictions d'accès strictes). En outre, certaines bases de données peuvent être consultées directement par les services de police, comme le registre national, le registre des détentions et le registre central des armes.⁵⁷ Le présent règlement sur l'entraide policière n'est pas applicable si l'utilisation de moyens coercitifs est nécessaire pour obtenir les informations demandées. Dans ce cas, les informations ne sont pas directement disponibles ou accessibles.⁵⁸

Les données et informations peuvent être fournies de manière autonome par les forces de police aux forces de police des autres Etats membres, sans l'intervention d'une autorité judiciaire (art. 2/5, §1 EJI). La loi précise deux cas dans lesquels la transmission de données et d'informations n'est possible qu'avec l'autorisation écrite préalable de l'autorité judiciaire compétente (art. 2/5, §2 EJI). Le premier cas concerne la transmission de données et d'informations qui font l'objet d'une mesure d'embargo.⁵⁹ Le second cas concerne le transfert de données et d'informations qui, dans le cadre d'une procédure belge, ne peuvent être obtenues par les services de police qu'avec l'autorisation d'un magistrat.

La fourniture d'informations policières se fait sans préjudice des instruments juridiques internationaux relatifs à la coopération policière internationale par lesquels la Belgique est liée et qui visent à promouvoir cette coopération (art. 2/3 EJI). Cette disposition fait également référence aux accords ou conventions bilatéraux ou multilatéraux sur la coopération policière internationale qui permettent un échange plus large de données et d'informations policières.⁶⁰

En principe, l'Etat membre destinataire n'est pas autorisé à utiliser les informations obtenues comme preuve. Cette utilisation n'est possible que si une autorisation est obtenue auprès des autorités judiciaires belges (art. 2/4 EJI). En principe, une telle demande devrait être faite par le biais d'une demande d'entraide juridique classique, mais le magistrat compétent peut également ajouter à la transmission par le canal de la police explicitement une déclaration formelle au torisant l'utilisation de l'information comme preuve.⁶¹

En ce qui concerne la transmission (de façon autonome) par les services de police, la loi prévoit quatre motifs de refus impératifs (art. 2/6 EJI). Le premier motif de refus concerne une éventuelle atteinte aux intérêts de la sécurité nationale de l'Etat belge. Le deuxième motif de refus exige que le déroulé d'une enquête en cours puisse être compromis, à la discrétion de l'autorité judiciaire compétente. Le troisième motif rend la transmission impossible si cela peut mettre en danger la sécurité des personnes ou des sources. Selon l'exposé des motifs, les personnes comprennent les suspects, les témoins et les victimes, tandis que les sources de données et d'informations comprennent les informateurs. Le quatrième et dernier motif de refus concerne les transmissions qui sont disproportionnées ou non pertinentes par rapport aux objectifs pour lesquels les données et les informations seraient fournies.

Les autorités de police compétentes peuvent transmettre des données et des informations de leur propre initiative, et donc sans demande préalable, à une autorité de police d'un autre Etat membre de l'UE. Ces transmissions sont également appelées transmissions spontanées de données. Une transmission spontanée est possible s'il existe des raisons factuelles de croire que les données et informations pourraient contribuer au dépistage ou à la prévention ou à l'investigation des infractions visées à l'article 5 § 2 de la loi du 19 décembre 2003 relative au mandat d'arrêt européen (art. 2/7 Loi EJI). Il s'agit des 32 catégories d'infractions pour lesquelles le contrôle de la double incrimination n'est pas requis pour l'exécution d'un mandat d'arrêt européen.

56 Circulaire commune COL 2/2000 du ministre de la Justice et du Collège des Procureurs généraux, 14 février 2000, p. 2.

57 Exposé des Motifs, paragraphe 17 et la discussion de l'art. 4 à la page 14 ; COL 01/2016 paragraphe 2.2.

58 Exposé des Motifs, p. 14-15.

59 Tel que visé à l'article 44/8 de la loi du 5 août 1992 sur la fonction de police ou à l'article 11 de la loi du 10 juillet 2006 relative à l'analyse de la menace.

60 COL 01/2016 paragraphe 2.6.

61 COL 01/2016 paragraphe 2.5.

Loi sur la fonction de police, modifiée par la Loi sur la gestion de l'information policière

Juste avant la transposition de la Décision-cadre suédoise par la loi sur l'entraide judiciaire que nous venons d'évoquer, la loi sur la gestion de l'information policière du 18 mars 2014.⁶² a été insérée dans la loi sur la fonction de police un cadre général sur le traitement des données dans le contexte de la coopération judiciaire et policière internationale en matière d'échange d'informations. Les articles 44/11/6 et 44/11/13, insérés respectivement par les articles 29 et 36 de la loi sur la gestion de l'information policière, sont pertinents à cet égard. L'article 44/11/6 prévoit que la transmission d'informations judiciaires est soumise à l'autorisation de l'autorité judiciaire compétente. Comme cela est clairement incompatible avec ce qui découle de la Décision-cadre suédoise, une exception est ajoutée à cet article pour les cas visés au chapitre I de la loi sur l'entraide judiciaire.⁶³ En effet, la Décision-cadre pose en règle l'absence d'autorisation judiciaire obligatoire avant transmission.⁶⁴ En outre, l'article 36 de la loi sur la gestion de l'information policière a été inséré dans l'article 44/11/13 de la loi sur la fonction de police, qui définit un cadre juridique pour le partage (ou la transmission) de données et d'informations à caractère personnel aux forces de police étrangères et aux organisations internationales. Pour les divulgations aux forces de police de l'UE, cette disposition n'est pertinente que si le pays destinataire souhaite aller au-delà de ce qui est déjà prévu par la législation européenne.⁶⁵

L'échange de données judiciaires

L'échange d'informations judiciaires est basé sur une demande classique d'entraide judiciaire. Le deuxième chapitre de la loi EJI, sur les principes généraux de l'entraide judiciaire internationale en matière pénale, s'y applique. Les demandes d'entraide judiciaire belges à destination d'autres États membres de l'UE sont envoyées directement aux autorités judiciaires de l'État requis. Les demandes provenant d'autres États membres peuvent être transmises aux autorités judiciaires compétentes par l'intermédiaire du Service public fédéral Justice, mais sont généralement reçues directement par elles.⁶⁶ Par dérogation à l'article 873, alinéa 2 du Code judiciaire, en vertu de l'article 5, alinéa 1 de l'EJI, l'exécution des demandes d'entraide judiciaire émanant d'autres États membres de l'UE ne requiert pas l'autorisation du Ministre de la Justice. Toutefois, conformément à l'obligation d'information prévue à l'article 7, §3 de l'EJI, le Service public fédéral Justice doit être informé de toute demande envoyée et reçue directement, par le biais d'une copie. Cette transmission au ministre peut se faire directement.⁶⁷

La législation belge ne régleme que les motifs de refus pour les demandes d'entraide judiciaire qui ne relèvent pas du champ d'application d'un instrument juridique international sur l'entraide judiciaire en matière pénale (Art. 4 EJI). Si la Belgique est liée par un traité ou un accord bilatéral d'entraide judiciaire, seuls les motifs de refus mentionnés dans ce traité ou cet accord sont applicables.⁶⁸ Pour les demandes d'entraide judiciaire émanant d'autres États membres, le cadre judiciaire européen est donc principalement applicable. En vertu de l'article 7, §4 de l'EJI, l'obligation de fournir des informations est plus stricte si la demande envoyée ou reçue par une autorité judiciaire belge concerne une question susceptible de troubler gravement l'ordre public ou de porter atteinte aux intérêts essentiels de la Belgique. Dans ce cas, le ministre de la Justice doit recevoir un rapport d'information plus détaillé. Celui-ci est envoyé sans délai par le procureur fédéral ou, si un juge d'instruction ou un procureur général est chargé de la demande, par le procureur général. Cette obligation d'information s'applique sans préjudice de l'obligation spécifique d'information prévue à l'article 5, qui stipule que l'autorité judiciaire requise doit transmettre la demande reçue au Ministre de la Justice si l'exécution peut être refusée soit parce qu'elle porte atteinte à la souveraineté, à la sécurité ou à l'ordre public ou à d'autres intérêts essentiels de la Belgique, soit parce que la demande concerne des infractions politiques. Si la demande est reçue par un procureur du Roi ou un juge d'instruction, elle est transmise au ministre de la Justice avec l'intervention du Procureur général (art. 5, 2ème al. EJI). En pratique, les autorités judiciaires belges peuvent envoyer les dossiers au Service public fédéral Justice, Direction générale de la législation / Droits fondamentaux et libertés, Service de la coopération internationale pénale. Le Service public fédéral veillera

62 Innovations dans la loi sur la fonction de police et la loi sur l'assistance judiciaire en ce qui concerne l'échange international d'informations policières, p. 199

63 Inséré avec l'art. 11 de la loi du 15 mai 2014.

64 Art. 3, 4ème al., Décision-cadre suédoise.

65 P. de Hert et al, " Vernieuwingen in de wet politieambt en de rechtshulpwet met betrekking tot de internationale uitwisseling van politie informatie ", *Vigiles* 2016/5, p. 200-201.

66 Circulaire conjointe du ministre de la Justice et du Collège des procureurs généraux du 9 février 2005 relative à l'entraide judiciaire internationale en matière pénale, p. 16.

67 COL 5/2005, p. 16.

68 COL 5/2005, p. 5.

à ce que les documents soient soumis au cabinet du ministre de la Justice.⁶⁹ Dès réception, le ministre doit informer l'autorité requérante que la demande ne peut être satisfaite en tout ou en partie. Cette information est également communiquée à l'autorité judiciaire concernée et fait obstacle à l'exécution de la demande d'entraide ou au retour des pièces d'exécution (art. 5, 3^{ème} al. EJI).

Les documents demandés sont envoyés directement, et non via le Service public fédéral Justice, à l'autorité judiciaire de l'État membre requérant. Cette transmission doit également avoir lieu directement si la demande a été initialement reçue par l'autorité centrale belge.⁷⁰ Si une demande ne peut être exécutée, ou ne peut être exécutée dans le délai prescrit, l'autorité belge compétente en la matière en informera sans délai l'autorité étrangère compétente (art. 6 §4 EJI).

Loi sur le traitement des données personnelles

Le législateur belge a transposé la directive sur les enquêtes et les poursuites dans la loi sur le traitement des données à caractère personnel du 30 juillet 2018 (ci-après « loi protection des données »). Cette loi-cadre succède à la loi sur la protection de la vie privée du 8 décembre 1992 et contient également d'autres dispositions d'application du RGPD. Le titre 2 de la loi protection des données prévoit la transposition de la directive relative aux recherches et aux poursuites et régit le traitement des données à caractère personnel par les autorités judiciaires et policières. Conformément à l'article 27 de la loi protection des données, ce titre s'applique au traitement des données à caractère personnel par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. La base juridique du traitement des données de police se trouve à l'article 44/1 de la loi sur la fonction de police. Celle-ci stipule que les services de police doivent traiter les informations et les données personnelles conformément aux objectifs de l'article 27 de la loi protection des données. Des conditions supplémentaires sont prévues pour des catégories spécifiques de données personnelles (données biométriques, données de santé, données génétiques). L'article 29, §4, de la loi protection des données stipule qu'aucune condition plus stricte que celles applicables au transfert national des données ne peut être attachée aux transferts vers d'autres États membres de l'UE.

3.2.2 Échange international de renseignements fiscaux

Les règlements de l'UE sur l'échange d'informations ont été mis en œuvre en Belgique dans diverses lois fiscales. Il s'agit du Code de l'impôt sur le revenu (CIR 92), du Code des droits d'enregistrement, d'hypothèque et greffe, du Code des droits de succession et du Code des droits et taxes divers. Les dispositions contenues dans le Code des impôts sur le revenu sont décrites ci-dessous.

Le principe de base en droit belge est le secret, comme l'exprime l'article 337 du Code des impôts sur les revenus. « Celui qui intervient, à quelque titre que ce soit, dans l'application des lois fiscales ou qui a accès dans les bureaux de l'administration chargée de l'établissement, ou celle en charge de la perception et du recouvrement, des impôts sur le revenu, est tenu de garder, en dehors de l'exercice de ses fonctions, le secret le plus absolu au sujet de tout ce dont il a eu connaissance par suite à l'égard de toutes les questions dont il a connaissance par suite de l'exécution de sa mission. »

Contrairement aux législations allemande et néerlandaise, la législation fiscale belge concernant la transposition de la Directive 2011/16/UE et des modifications ultérieures est particulièrement complexe et donc difficile à résumer en quelques mots. L'autorité compétente belge échange des informations avec les autorités compétentes étrangères (art. 338, al. 3). Conformément à la réglementation européenne, la législation belge prévoit également la transmission d'informations sur demande et l'échange spontané. À la demande d'une autorité compétente étrangère, l'autorité compétente belge fournit toutes les informations énumérées au premier alinéa qu'elle a en sa possession ou qu'elle a obtenues à la suite d'une enquête administrative nécessaire à l'obtention de ces informations (art. 338, al. 5). Bien entendu, l'échange automatique d'informations est également rendu possible (art. 338, al. 6/1).

La communication spontanée d'informations est prévue à l'alinéa 7. L'autorité compétente belge fournit spontanément des informations à une autorité compétente étrangère et énumère les conditions dans

⁶⁹ COL 5/2005, p. 14.

⁷⁰ COL 5/2005, p. 16.

lesquelles cette communication peut avoir lieu. L'une des conditions est que ces informations doivent être suffisantes, pertinentes et non excessives pour cette autorité. Les alinéas 9 et 10 permettent aux fonctionnaires belges autorisés d'être présents dans les bureaux où les autorités administratives de l'État membre requis exercent leurs fonctions et d'être présents lors des enquêtes administratives sur le territoire de l'État membre requis (art. 338, al. 9). Il en va de même pour les fonctionnaires étrangers sur le territoire belge (art. 338, al. 10). En Belgique, les agents étrangers ne peuvent pas interroger les personnes ni examiner les documents.

Les informations ne peuvent être échangées qu'au cours de procédures judiciaires et administratives susceptibles de déboucher sur une sanction pour infraction fiscale, sans préjudice des règles et dispositions générales relatives aux droits des prévenus et des témoins dans ces procédures (art. 338, par. 17, al. 2). Avec l'autorisation de l'autorité compétente étrangère qui a communiqué les informations conformément à la directive et pour autant que la loi belge l'autorise, les informations et documents reçus de cette autorité peuvent être utilisés à des fins autres que celles visées au deuxième alinéa. Les informations peuvent également être transmises à un État membre tiers, la Belgique ayant choisi le système en vertu duquel l'État membre expéditeur est réputé avoir donné son consentement s'il ne s'y oppose pas dans un délai de dix jours. Le consentement est cependant requis si les informations doivent être utilisées dans le cadre d'une procédure pénale. L'autorité compétente belge peut autoriser l'utilisation des informations et documents communiqués conformément aux dispositions de la présente législation par l'État membre qui les reçoit, à des fins autres que le recouvrement des créances relatives à certains impôts, taxes et autres mesures et l'établissement et le recouvrement des cotisations obligatoires de sécurité sociale. L'autorité compétente belge donne son accord à condition que leur utilisation soit possible en Belgique à des fins similaires (art. 338, al. 18).

La communication d'informations aux autorités étrangères est soumise aux conditions habituelles, telles que la règle de l'épuisement, le principe de réciprocité, la non-violation de secrets d'affaires et d'autres intérêts commerciaux, ainsi que la contrariété à l'ordre public (art. 338, al. 19 et art. 338, al. 20). Le paragraphe 20 introduit la restriction selon laquelle la communication d'informations relatives aux périodes imposables antérieures au 1^{er} janvier 2011 peut être refusée si elle aurait pu l'être sur la base de la directive 77/799/CE, c'est-à-dire si une enquête est nécessaire.⁷¹

3.2.3 Échange international d'informations administratives

En Belgique, le règlement général sur la protection des données 2016/79/UE a été intégré dans la loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel, datée du 30 juillet 2018. Cette loi a transposé les lois, décrets et ordonnances sectoriels existants. L'article 29, alinéa 1, indique que le traitement ultérieur par le même ou un autre responsable du traitement pour une finalité énumérée à l'article 27, autre que celle pour laquelle les données à caractère personnel ont été collectées, est autorisé. Les conditions sont que le responsable du traitement soit autorisé par la loi, un décret, une ordonnance, le droit de l'Union européenne ou un accord international à traiter ces données personnelles pour une telle finalité ; et que le traitement soit nécessaire et proportionné conformément à la loi, au décret, à l'ordonnance, au droit de l'Union européenne ou à l'accord international. L'article 27 concerne le traitement de données à caractère personnel par les autorités compétentes aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Si tel n'est pas le cas, les données à caractère personnel ne peuvent pas être traitées ultérieurement par le même ou un autre responsable du traitement (art. 29, al. 2). Les conditions applicables aux échanges au niveau national s'appliquent également aux transmissions à des destinataires situés dans les autres États membres de l'Union européenne (art. 29, al.4).

⁷¹ Directive du Conseil du 19 décembre 1977 concernant l'assistance mutuelle des autorités compétentes des États membres dans le domaine des impôts directs. Journal officiel des Communautés européennes. No. L336/15.

3.3 Les cadres juridiques nationaux en Allemagne

3.3.1 Échange international d'informations en matière pénale

Gesetz über die Internationale Rechtshilfe in Strafsachen (loi sur l'entraide judiciaire internationale en matière pénale)

L'entraide judiciaire en matière pénale entre l'Allemagne et d'autres pays est régie par la *Gesetz über die Internationale Rechtshilfe in Strafsachen* (IRG)⁷² et expliquée plus en détail dans les *Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten* (RiVAST). Toutefois, le RiVAST ne s'applique que dans la mesure où il ne viole pas les traités internationaux et, en outre, il est possible d'y déroger dans des cas particuliers (n° 1, al. 1, RiVAST).

Conformément à l'article 92 de l'IRG, les services de police fédéraux et des États fédérés compétents sont autorisés à fournir des informations, y compris des données à caractère personnel, à la demande d'un service répressif⁷³ d'un État membre de l'UE. La transmission doit avoir lieu dans le but de poursuivre des infractions et est soumise aux mêmes conditions juridiques que celles qui s'appliquent aux autorités de police allemandes, sans préjudice des dispositions du §3 du *Bundeskriminalamtgesetz* (BKAG) sur la coopération internationale (Art. 92, al.1 IRG).⁷⁴ Toutefois, la partie destinataire n'est pas autorisée à utiliser les informations fournies comme preuve dans une procédure judiciaire, à moins que l'autorité compétente n'ait donné son accord (art. 92, al. 2 IRG).

Cette disposition comprend certains motifs de refus obligatoires et facultatifs. Tout d'abord, il n'est pas permis de fournir des données si cela porte atteinte aux intérêts essentiels de la sécurité de la Fédération ou des États fédérés, si des mesures coercitives sont nécessaires pour obtenir les informations demandées ou si la transmission des informations est disproportionnée ou non pertinente au regard des finalités pour lesquels elles sont demandées (Art. 92, al. 3 IRG). Elle prévoit également qu'une demande peut être refusée si l'information demandée n'est pas en possession de l'autorité requise et que cette information ne peut être obtenue sans recourir à des mesures coercitives, si le succès d'une enquête en cours ou la sécurité des personnes en serait compromise, ou si l'infraction à laquelle la transmission se rapporte est punie en droit allemand d'une peine privative de liberté d'un an ou moins (art. 92, al. 4 IRG).

L'échange spontané de données avec les États membres de l'UE est régi par l'article 92c de l'IRG. Cette disposition permet aux autorités publiques de divulguer des données à caractère personnel aux autorités publiques d'autres États membres sans demande préalable lorsqu'il existe un soupçon d'infraction pénale. Bien que l'article 92 IRG ne concerne que les autorités de police, une divulgation au titre de l'article 92c IRG peut être effectuée par toutes les autorités publiques allemandes (*öffentliche Stellen*), comme le prévoit l'alinéa 2 de la *Bundesdatenschutzgesetz*.⁷⁵ Cette disposition s'applique donc, entre autres, au ministère public, aux autorités judiciaires, à la police et aux autorités douanières.⁷⁶

La transmission spontanée ne peut avoir lieu que si elle est possible sans demande à un tribunal ou à un procureur allemand et si elle est utile à l'engagement d'une procédure pénale dans l'autre État membre ou à la poursuite d'une procédure pénale déjà engagée (art. 61a, al.1 IRG). Les conditions énoncées à l'article 61 bis, alinéas 2 à 4, pour la transmission d'informations sur demande s'appliquent *mutatis mutandis*. Par exemple, les délais prévus par la législation allemande pour la destruction des données doivent être respectés et les données transmises ne peuvent être utilisées que dans le but pour lequel elles ont été transmises (art. 61a, al. 2, points a) et b) de l'IRG).

72 Dans la mesure où l'IRG ne contient pas de dispositions procédurales spécifiques, les dispositions des *Gerichtsverfassungsgesetzes* et de ses *Einführungsgesetzes*, du *Strafprozeßordnung*, des *Jugendgerichtsgesetzes*, de l'*Abgabenordnung* et des *Gesetzes über Ordnungswidrigkeiten* s'appliquent par analogie (§77 I IRG).

73 Comme indiqué à l'article 2, point a), de la décision-cadre suédoise.

74 La fourniture de données à caractère personnel par le service fédéral allemand de police criminelle est régie par le BKAG et expliquée plus en détail au chapitre 4.

75 République fédérale d'Allemagne, *Spontaneous sharing of information pursuant to sections 61a, 92c of the Act on International Cooperation in Criminal Matters [Gesetz über die internationale Rechtshilfe in Strafsachen, IRG]*, juin 2017, p. 2.

76 D. Van Daele & B. Vangeebergen (2007). *Criminaliteit en rechtshandhaving in de Euregio Maas-Rijn*, deel 2. Intersentia, p. 736.

L'échange de données de police

La police en Allemagne se compose des forces de police des seize États fédérés allemands, des forces de police fédérales (*Bundespolizei*), du département fédéral d'enquête criminelle (*Bundeskriminalamt*) et de la police parlementaire (*Polizei beim Deutschen Bundestag*). L'article 30 GG (Grundgesetz für die Bundesrepublik Deutschland) stipule que l'exercice des compétences étatiques et l'accomplissement des tâches étatiques appartiennent aux États fédérés, à moins que la Constitution ne prévoise ou n'autorise une disposition différente. Dans la mesure où la Constitution ne confère pas cette compétence à la Fédération, le pouvoir législatif appartient aux États fédérés en vertu de l'article 70, al 1 GG. Le pouvoir législatif général en matière de (fonction de) police n'étant pas explicitement attribué, cette compétence revient en principe aux États fédérés.⁷⁷

La police en Allemagne étant au premier chef organisée au niveau fédéré, chaque État fédéré dispose de sa propre législation sur l'organisation et les pouvoirs de la police.⁷⁸ Les forces de police des États fédérés sont subdivisées en plusieurs services, dont la *Kriminalpolizei* est le plus pertinent dans le contexte de ce précis. La *Kriminalpolizei* est le service d'enquête criminelle allemand et s'occupe des enquêtes sur les infractions pénales (plus graves).⁷⁹

En vertu de l'article 73 GG, certaines compétences législatives dans le domaine du droit de la police sont exclusivement attribuées à la Fédération, notamment la coopération entre la Fédération et les États fédérés en matière d'enquêtes pénales, la création d'une police fédérale d'investigation et la lutte internationale contre la criminalité (art. 73, al. 1, point 10 du BKAG).

Bundeskriminalamt

Le *Bundeskriminalamt* (ou l'*Office fédéral de police criminelle*) (BKA) fait partie du ministère fédéral de l'Intérieur (art. 1, al. 1 du BKAG). La police judiciaire fédérale est le service central d'information et de renseignement de la police et soutient les forces de police de la Fédération et des États fédérés dans la prévention et la poursuite des délits qui dépassent les frontières d'un État fédéré ou qui revêtent une dimension internationale ou une importance signative de quelque autre ordre que ce soit (art. 2, al. 1 BKAG). Chaque État fédéré dispose d'un *Landeskriminalamt* (LKA), qui fait office de bureau central et de lien entre les services de police judiciaire locaux et le BKA (art.1, al. 2 du BKAG).

Le BKA est le bureau central national de la République fédérale d'Allemagne pour Interpol et l'unité nationale pour Europol. Le BKA est également l'agence centrale allemande pour l'échange d'informations pour la gestion de la partie nationale du système d'information Schengen et le bureau SIRENE pour l'échange d'informations supplémentaires (paragraphe 3, deuxième alinéa, BKAG). Le BKA est également chargé de la communication officielle nécessaire avec les autorités policières et judiciaires et les autres organismes publics compétents des États étrangers aux fins de la prévention ou de la poursuite des infractions pénales (paragraphe 3, troisième alinéa, du BKAG). Les services de police des États fédéraux sont également autorisés à le faire, si la communication a lieu avec les pays voisins et les États membres de l'UE, dans la mesure où elle concerne la criminalité dans la zone frontalière à caractère régional, ou dans la mesure où il y a une nécessité urgente (*Gefahr im Verzug*). Le BKA doit toutefois être immédiatement informé de cette prise de contact par le service de police compétent (art.3, al. 4 du BKAG).

La communication de données à caractère personnel par le BKA est régie à la section 2.3 de *Bundesdatenschutzgesetz* (BKAG). Cette section comporte des dispositions distinctes pour l'échange d'informations au niveau national (art. 25 du BKAG) et pour les communications au sein de l'UE (par. 26 du BKAG) et aux pays tiers et aux organisations internationales (art. 27 du BKAG). La responsabilité de la communication d'informations aux États membres de l'UE incombe au BKA (art. 26, al.1 du BKAG).

Les données qui peuvent être traitées par les services participant au *Polizeilichen Informationsverbund* sont énumérées de manière exhaustive à l'article 30, alinéa 1 du BKAG. Il s'agit notamment des données à caractère personnel dont le traitement est nécessaire à la prévention et aux poursuites qui dépassent les frontières des

77 D. van Daele, T. Spapens & C. Fijnaut (2008). De strafrechtelijke rechtshulpverlening van België, Duitsland en Frankrijk aan Nederland. Intersentia, p173.

78 Van Daele, Spapens & Fijnaut 2008, p. 174.

79 Van Daele, Spapens & Fijnaut 2008, p. 174.

Etats fédérés, de nature internationale, d'infractions pénales, ou de nature particulièrement grave, ainsi que des données à caractère personnel dont le traitement est nécessaire à des fins d'identification ou de recherche de personnes et de choses.

La réglementation des échanges d'informations au niveau national contenue dans le paragraphe 25 du BKAG s'applique *mutatis mutandis* à la divulgation de données personnelles aux États membres de l'UE (art. 26, al.1 point 1 du BKAG). Le BKA est responsable de l'admissibilité du transfert de données. Les dispositions relatives aux transferts de données dans le cadre de l'entraide judiciaire internationale en matière pénale et dans le cadre d'accords spéciaux de droit international restent pleinement applicables en vertu de l'article 26, alinéa 1 du BKAG.

Les interdictions de divulgation et les motifs de refus sont déterminés à l'article 28 du BKAG. En vertu de cette disposition, l'on s'abstient de communiquer des informations si l'intérêt légitime de la personne concernée l'emporte sur l'intérêt général. La communication n'est pas non plus autorisée si elle entre en conflit avec la loi fédérale. En outre, les obligations légales de confidentialité ainsi les obligations de confidentialité professionnelles ou liées à la fonction, même si elles ne font pas l'objet d'une loi, doivent toujours être respectées. Les transmissions aux États membres de l'UE sont également exclues si elles risquent de porter atteinte aux intérêts essentiels de la sécurité de l'État fédéral ou des États fédérés, de compromettre le succès d'une enquête en cours ou la vie, l'intégrité physique ou la liberté d'une personne, d'entrer en conflit avec les objectifs d'autres lois allemandes ou de contrevenir aux principes énoncés dans la Charte des droits fondamentaux de l'Union européenne.

Bundespolizei

La *Bundespolizei* fait partie du ministère fédéral de l'Intérieur et a un large éventail de tâches liées à la sécurité nationale. La *Bundespolizei* est notamment chargée du contrôle des frontières, de la police ferroviaire et de la sécurité aérienne. Dans l'exercice de ces missions, elle est également chargée de la lutte contre la criminalité. Les tâches et les pouvoirs de la *Bundespolizei* sont principalement régis par la *Bundespolizeigesetz* (BPolG). Conformément à l'article 32a, premier al., la *Bundespolizei* peut, à la demande d'une autorité répressive, telle que visée à l'article 2, point a), de la Décision-cadre suédoise, transférer des données à caractère personnel à d'autres États membres de l'UE aux fins de la prévention des infractions pénales (art. 32a, al. 5 de la BPolG). Cette demande doit contenir les informations énumérées au deuxième alinéa. Le troisième alinéa permet la communication spontanée de données si, dans un cas précis, il existe un risque qu'une infraction au sens de l'article 2, alinéa 2, de la Décision-cadre relative au mandat d'arrêt européen soit commise et s'il existe des indices concrets que la communication de ces données à caractère personnel pourrait contribuer à prévenir cette infraction pénale.

Les dispositions relatives à la transmission de données au niveau national s'appliquent *mutatis mutandis* aux transmissions vers d'autres États membres de l'UE (art. 32a, al. 1 et 3, BPolG). Outre l'interdiction générale de transmission prévue à l'article 33, alinéa 3 BPolG, les alinéas 3a et 3b énumèrent quelques motifs supplémentaires de refus de transmission aux États membres de l'UE.

Il est également toujours possible à la *Bundespolizei* de transmettre des données à caractère personnel à un service de police ou à une autre autorité publique d'un État membre de l'UE sur la base de l'article 32, 2ème al. ou sur la base d'accords spéciaux en vertu du droit international. Le troisième paragraphe de l'article 32 permet de transmettre des données à caractère personnel aux autorités publiques d'autres États si cela est nécessaire à l'exécution de la mission de la *Bundespolizei*, à la prévention d'un danger grave ou à la lutte contre des crimes d'importance majeure. Un motif supplémentaire de refus pour de telles transmissions se trouve à l'article 33, alinéa 3 du BPolG.

L'échange d'informations judiciaires

Le *Bundesamt für Justiz* (ou *Office judiciaire fédéral*) (BfJ) est le prestataire central de la justice et le point de contact pour les transactions juridiques internationales. En outre, le BfJ fait office de point de contact au sein du Réseau judiciaire européen en matière pénale et de point de contact pour Eurojust. La BfJ est une *Bundesoberbehörde* (*Autorité fédérale supérieure*) qui relève de la responsabilité du *Bundesministeriums der Justiz und für Verbraucherschutz*.

Conformément à l'article 1 de la *Bundeszentralregistergesetz (loi sur le registre central fédéral)* (BZRG), le *Bundeszentralregister* (BZR) est géré par le BfJ. Il enregistre, entre autres, les condamnations pénales prononcées par les tribunaux allemands et, si les conditions applicables sont remplies, également les condamnations étrangères d'Allemands et de personnes nées ou résidant en Allemagne (voir art. 4 et art. 54 BZRG). Les dispositions relatives à l'échange d'informations issues du BZR au sein de l'UE figurent à l'article 57a de la BZRG. Selon le premier article, les informations sur les condamnations des personnes ayant la nationalité d'un autre État membre de l'UE doivent être recueillies et transmises à l'autorité compétente de l'État membre de la nationalité du condamné. Si la personne a plusieurs nationalités européennes, les informations doivent être transmises à chaque État membre concerné (art.57 l a BZRG). Si une demande est reçue d'un autre État membre concernant la transmission d'informations disponibles du BZR en appui d'une procédure pénale, cette demande doit être exécutée par le BfJ conformément au deuxième alinéa (art. 57a, al. 2. BZRG). L'article 84 RiVAST prévoit également qu'une demande d'entraide judiciaire qui ne peut être exécutée qu'en obtenant des informations du BZK doit être soumise directement au BfJ. Si, en plus de la demande d'informations du BZK, une autre entraide judiciaire est également demandée, une copie de la demande doit être envoyée directement au BfJ. Le BfJ transmet ensuite les informations du registre demandées à l'autorité requise pour transmission ou l'informe des obstacles éventuels.

Bien que le pouvoir de décider des demandes d'entraide judiciaire en provenance et à destination de pays étrangers incombe en premier lieu au gouvernement fédéral en vertu de l'article 74, alinéa 1 de l'IRG, l'exercice de ce pouvoir peut être transféré aux gouvernements des États fédérés en vertu du deuxième paragraphe. Le BfJ, dans la mesure où la compétence n'a pas été déléguée aux États fédérés, a le pouvoir de décision d'accéder aux demandes d'entraide judiciaire entrantes et sortantes en matière pénale. Toutefois, si la demande concerne un État membre de l'UE, cette compétence est déléguée aux gouvernements des États fédérés en vertu de la *Zuständigkeitsvereinbarung*.⁸⁰ Comme les *Landesregierungen* ont à leur tour délégué ce pouvoir, la procédure exacte de décision diffère d'un État fédéré à l'autre (art. 74, al.2 IRG).

Rhénanie du Nord-Westphalie

Le RiVAST stipule que la *Bewilligungsbehörde* est responsable de l'évaluation des demandes d'entraide judiciaire entrantes et sortantes (art. 7, l, a RiVAST). La *Bewilligungsbehörde* applicable se trouve dans la législation de l'État fédéré. Pour l'Euregio Meuse-Rhin, c'est l'État fédéré de Rhénanie du Nord - Westphalie qui est pertinent, où la compétence en matière d'entraide judiciaire avec les pays étrangers en matière pénale est régie par le GRdE-RHSt.⁸¹ La compétence pour répondre aux demandes d'entraide judiciaire reçues dans le cadre de l'échange d'informations avec les États membres de l'UE est en principe attribuée au *Staatsanwaltschaft* (ministère public) localement compétent (art..1.1.2.1. GRdE-RHSt).

Un règlement distinct est en place pour les demandes d'informations de la police (voir les art.2.1 et 2.2. GRdE-RHSt). Ce règlement est précisé dans la *Polizeiorganisationgesetz Nordrhein-Westfalen* (POG NRW) et la *Polizeigesetz des Landes Nordrhein-Westfalen* (PolG NRW). Le rôle et les tâches du LKA Nordrhein-Westfalen sont régis par l'article 13 du POG NRW et par l'ordonnance du 7 mai 2003.⁸² Le LKA joue un rôle important dans le domaine de la coopération internationale en matière pénale. Il s'agit de l'agence principale (*Prüfungs- und Bewilligungsbehörde*) pour les demandes d'assistance judiciaire entrantes et sortantes de la police et elle coordonne également les intérêts de la police en matière d'entraide judiciaire.⁸³

⁸⁰ Vereinbarung zwischen der Bundesregierung und den Landesregierungen von Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein et Thüringen über die Zuständigkeit im Rechtshilfeverkehr mit dem Ausland in strafrechtlichen Angelegenheiten (Zuständigkeitsvereinbarung 2004).

⁸¹ Exécution de la compétence en matière pénale, obligations de déclaration et coopération au sein du réseau judiciaire européen et avec les réseaux transnationaux Réponse commune à la question de savoir si le ministère de la Justice - 9350 - III. 19 -, des Ministeriums für Inneres und Kommunales - 424 - 57.01.48 - und des Finanzministeriums - S 1320 - 5 - V B 5/ S 770 - 4 - V A 1 - von 16. Dezember 2016 - JMBL. NRW S. 16 (GRdE-RHSt).

⁸² Verordnung über weitere polizeiliche Aufgaben des Landeskriminalamts bei der Gefahrenabwehr sowie der Erforschung und Verfolgung von Straftaten du 26. Novembre 2020.

⁸³ Voir art. 7, al. 1, Verordnung über weitere polizeiliche Aufgaben des Landeskriminalamts bei der Gefahrenabwehr sowie der Erforschung und Verfolgung von Straftaten du 26 novembre 2020; Politikunde 50 Recherchesamenwerking in de Euregio Maas-Rijn, p. 40 ; art. 2.1.2.1 GRdE-RHSt.).

Le LKA fait également office de point de contact central pour les pays étrangers dans le cadre de la coopération policière transfrontalière et de la coopération avec Europol.⁸⁴

Les règles relatives à la transmission de données sont définies au titre 3 de la PolG NRW. Comme le BKAG, la PolG NRW prévoit des réglementations distinctes pour l'échange national d'informations (art. 27) et pour les transferts de données au sein de l'UE (art. 28) ainsi que vers des pays tiers et des organisations internationales (art. 29). La disposition de l'article 27 PolG NRW sur l'échange d'informations au niveau national s'applique *mutatis mutandis* à la fourniture de données au sein de l'UE (art. 28, al. 1 PolG NRW). Le premier article stipule que les données à caractère personnel peuvent être échangées entre les services de police dans la mesure nécessaire à l'accomplissement de leurs propres tâches ou de celles du destinataire. Le transfert à une autre fin que celle pour laquelle les données ont été obtenues ou stockées n'est pas autorisé pour les données collectées en vertu de l'article 11.

Le deuxième article stipule que la transmission à d'autres autorités et à d'autres organismes publics est possible dans la mesure où cela est prévu par une autre disposition légale ou dans la mesure où la transmission est nécessaire à l'exercice de la fonction de police, à la prévention d'un danger ou à la prévention ou à la réparation d'une atteinte grave à l'intérêt public ou aux droits d'une personne.

Le troisième alinéa permet de transférer des données à caractère personnel à des personnes ou services non publics dans la mesure où cela est nécessaire à l'exécution de la mission de police, à la prévention d'un danger par le service destinataire, ou à la prévention ou à la réparation d'une atteinte grave à l'intérêt public ou aux droits d'une personne. La transmission est également possible si un intérêt légal est démontré et qu'il n'y a aucune raison de penser que les intérêts à protéger de la personne concernée l'emportent, ou si la transmission est clairement dans l'intérêt de la personne concernée et que celle-ci y consentirait si elle en avait connaissance.

En vertu de l'article 2.2.1.1 GRdE-RHSt, les forces de police sont autorisées à transmettre aux autorités requérantes, dans les mêmes conditions que celles applicables aux forces de police nationales, les informations déjà en leur possession ou auxquelles elles ont accès. Cela inclut les informations obtenues précédemment au moyen de mesures coercitives. Ce pouvoir s'applique en particulier aux catégories d'informations suivantes:

Certificats de transport et de propriété de véhicules terrestres, maritimes et aériens ;

- a. Informations sur les permis de conduire, les permis de navigation et autres documents similaires ;
- b. Lieux de résidence et de séjour ;
- c. Permis de séjour, passeports et cartes d'identité ;
- d. Propriétaires et utilisateurs de réseaux de télécommunications et de données ;
- e. Dispositions relatives à l'identité;
- f. Recherche de l'origine des objets (questions sur le parcours de vente) ;
- g. Informations provenant de collectes de données officielles (détenues en Allemagne) ;
- h. Déterminer la volonté d'individus à faire des dépositions ;
- i. Les interrogatoires de police ;
- j. Inspection, sécurisation et documentation des pistes existantes, et ;
- k. Informations sur les personnes en détention.

En sont exclues, entre autres, les informations qui ne peuvent être obtenues que sur la base d'une mesure de procédure pénale (Voir art. 2.2.1.2 GRdE-RHSt). Conformément à l'article 30, alinéa 3 de la PolG NRW, la Police NRW peut également adresser une demande aux autorités publiques des États membres de l'UE, pour autant que les conditions de collecte des données soient remplies et qu'il n'en soit pas disposé autrement par la loi.

La coopération avec les Pays-Bas et la Belgique au sein du Bureau de coopération eurégional en matière pénale (BES) est réglementée séparément dans le GRdE-RHSt (art. 3.2). En cas de problèmes dans la coopération transfrontalière en matière pénale, notamment dans les Eurégio Meuse-Rhin et Rhin-Meuse-Nord, il faut demander l'aide de la personne de contact en Rhénanie-du-Nord-Westphalie au BES (art.3.2.2 GRdE-RHSt). Le *Generalstaatsanwaltschaft* Düsseldorf (bureau du procureur général) est le point de contact du European Judicial Network EJN (art 3.1.1 GRdE-RHSt).

⁸⁴ Art. 7, al. 2, Verordnung über weitere polizeiliche Aufgaben des Landeskriminalamts bei der Gefahrenabwehr sowie der Erforschung und Verfolgung von Straftaten du 26 novembre 2020.

3.3.2 Échange international d'informations fiscales

Abgabenordnung 1977

Les conditions de l'échange de données fiscales avec les États membres de l'UE ont été mises en œuvre en Allemagne dans le code fiscal de 1977 (*Abgabenordnung, AO*). Les possibilités sont exposées à l'article 117 AO. Cet article permet aux autorités financières (*Finanzbehörden*) de fournir une assistance juridique et administrative aux autres États, dans le cadre du droit allemand (art. 117, al.1 AO). Les accords internationaux applicables ainsi que les règlements de l'UE en matière d'assistance mutuelle en constituent la base (art. 117, al.2 AO). En outre, cette assistance juridique peut être fournie dans d'autres cas, moyennant le respect d'un certain nombre de conditions. Tout d'abord, la réciprocité doit être assurée. Deuxièmement, l'État requérant doit garantir que les renseignements fournis ne seront utilisés que dans le cadre de procédures fiscales ou pénales (y compris les procédures relatives à des infractions administratives) et que les renseignements et documents fournis ne seront mis à la disposition que des personnes, autorités ou tribunaux impliqués dans le traitement du dossier fiscal ou dans la poursuite de l'infraction fiscale. Troisièmement, l'État requérant doit être prêt à éviter toute double imposition dans le cas des impôts sur le revenu, les bénéfices et le capital par accord mutuel, grâce à une délimitation appropriée des bases d'imposition. Quatrièmement, l'exécution de la demande ne doit pas porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de l'État fédéral ou de ses collectivités territoriales, il ne doit pas y avoir de risque de dommage pour la partie nationale concernée qui soit incompatible avec l'objet de l'assistance juridique et administrative, et la demande ne doit pas conduire à la divulgation de secrets commerciaux, d'affaires, industriels ou professionnels ou d'un processus de production ou de commerce. Si l'assistance juridique et administrative internationale concerne des impôts dont la responsabilité incombe aux autorités fiscales des États fédérés le ministère fédéral des finances (*Bundesministerium der Finanzen*) décide en concertation avec l'autorité supérieure compétente de l'État fédéré (art. 117, al. 3 AO).

L'article 117, alinéa 4 AO définit les pouvoirs des autorités fiscales et les droits et obligations des parties concernées et d'autres personnes, lorsqu'elles fournissent une assistance à un autre État. En vertu de l'article 1, alinéa 1 AO, les règles s'appliquent à tous les impôts, y compris les crédits d'impôt, prévus par le droit fédéral ou de l'Union européenne, dans la mesure où ils sont perçus par les autorités fiscales fédérales ou par les autorités fiscales des États fédérés. L'*Abgabenordnung* est exclusivement d'application en conformité au droit de l'Union européenne. En outre, l'assistance mutuelle est régie par le droit de l'État requérant en ce qui concerne l'appréciation de la recevabilité. Le droit de l'autorité requise s'applique à l'exécution (art. 114, al.1 de l'AO). L'autorité fiscale requérante est responsable à l'égard de l'autorité requise de la légalité de la mesure à prendre. L'autorité requise est responsable de l'exécution de l'assistance (art. 114, al.2 AO). L'article 91 AO s'applique également aux parties de droit allemand impliquées dans la transmission d'informations et de documents

Dans la mesure où l'assistance juridique ou administrative concerne des impôts qui relèvent de la compétence des autorités fiscales des États fédérés, la partie de droit allemand concernée est toujours entendue par dérogation à l'article 91, alinéa 1 AO, sauf s'il s'agit de taxes sur le chiffre d'affaires, s'il y a un échange d'informations sur la base de la réglementation de l'UE (directive 2011/16/UE) ou si une exception peut être faite sur la base de l'article 91, alinéa 2 ou 3 AO. Cette disposition stipule qu'il est possible de renoncer à une audition si elle n'est pas nécessaire dans les circonstances du cas d'espèce, en particulier lorsqu'une décision immédiate semble nécessaire en raison d'un danger imminent ou de l'intérêt public, lorsqu'il y a une collecte automatisée d'un grand nombre d'informations ou lorsque des mesures d'exécution doivent être prises (art. 91, al. 2 AO). En outre, aucune audition ne doit avoir lieu si elle est contraire à un intérêt public prépondérant (art. 91, al. 3 OA).

Les articles 117a et 117b AO contiennent certaines dispositions spécifiques concernant les enquêtes fiscales pénales. À la demande d'une autorité publique d'un État membre de l'UE chargée de la prévention et de la poursuite des infractions pénales, telle que désignée dans la Décision-cadre 2006/960/JAI, les autorités chargées des enquêtes fiscales peuvent fournir des données à caractère personnel liées aux tâches décrites à l'article 208 AO, dans le but de prévenir les infractions pénales. Cela concerne les enquêtes menées par la *Zollfahndung*. Les mêmes dispositions s'appliquent à la transmission d'informations qu'à la transmission au niveau national (art. 117a, al. 1 AO). Les demandes d'information doivent concerner des cas spécifiques et être soumises sous la forme d'une demande d'assistance juridique (par exemple, la description des faits, le but dans lequel les données sont demandées, les raisons de supposer que les informations demandées sont disponibles en Allemagne) (art. 117a, al. 2 AO). Des informations peuvent également être échangées spontanément à des fins de détection et de prévention, ou lorsqu'il existe un risque que des infractions visées

par le mandat d'arrêt européen soient commises⁸⁵, s'il existe des indices concrets que la communication de données à caractère personnel pourrait contribuer à la prévention d'une telle infraction (art. 117a, al. 3, OA).

La transmission spontanée d'informations est refusée lorsqu'elle est contraire aux conditions de transmission au niveau national ; lorsque, compte tenu de l'intérêt public particulier servi par la transmission, dans le cas d'espèce, la protection des intérêts de la personne concernée prévaut. Il s'agit notamment de protéger la vie privée de la personne concernée et de garantir un niveau adéquat de protection des données dans l'État destinataire. Les intérêts des personnes concernées dignes de protection peuvent également être sauvegardés par le fait que l'État destinataire ou l'organisme intergouvernemental ou supranational destinataire assure la protection des données dans des cas individuels (art. 117a, al. 4, OA). En outre, la communication (sur demande ou spontanée) ne doit pas porter atteinte aux intérêts essentiels de sécurité, ni contrevenir à l'article 6 du traité sur l'Union européenne. La communication des données est refusée si les données demandées ne sont pas disponibles auprès de l'autorité requise et ne peuvent être obtenues que par des mesures coercitives, ou lorsque la communication serait disproportionnée ou que les données ne sont pas nécessaires au regard de la finalité pour laquelle elles seraient transmises (art. 117a, al. 5 OA). En outre, la communication des données peut être refusée si les données demandées ne sont pas disponibles dans les bureaux des autorités fiscales chargées de l'enquête fiscale, mais peuvent être obtenues sans recourir à des mesures coercitives ; si cela risque de nuire à des enquêtes en cours, ou de mettre en danger la vie, l'intégrité physique ou la liberté d'une personne, ou si l'infraction pour la prévention de laquelle les données doivent être communiquées est punie par le droit allemand d'une peine d'emprisonnement maximale d'un an ou moins (art. 117a al. 6 AO).

Le paragraphe 117b AO précise que les informations fournies aux services des autorités d'enquête fiscale sur la base de la Décision-cadre 2006/960/JAI ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été transmises ou pour prévenir une menace réelle et sérieuse pour la sécurité publique. En outre, elles ne peuvent être utilisées à d'autres fins ou comme preuves dans des procédures judiciaires sans le consentement préalable de l'État communiquant. Les conditions d'utilisation des données imposées par l'État communiquant s'appliquent (art. 117b, al. 1 AO).

Zollfahndungsdienst

Le *Zollfahndungsdienst* fait partie de la *Zollverwaltung* (administration douanière allemande) et se compose du *Zollkriminalamt* et du *Zollfahndungsämtern* (art. 1 ZFdG 2021). Le *Zollkriminalamt* est le bureau central (*Zentralstelle*) du *Zollfahndungsdienst* et également l'un des bureaux centraux des douanes pour l'information et le renseignement (art.2 ZFdG 2021). Le *Zollfahndungsdienst* est chargé d'enquêter sur les infractions pénales et les infractions administratives relevant de la responsabilité des autorités douanières. Le *Zollfahndungsdienst* dispose de pouvoirs étendus tant en matière de *Gefahrenabwehr* (prévention) que de *Strafverfolgung* (répression) (voir les art. 3 et 4 de la ZFdG 2021). Le *Zollfahndungsdienst* traite des infractions douanières allant d'une gravité moyenne jusqu'à la criminalité organisée. Les principales activités sont réalisées par le *Zollfahndungsämtern*, qui s'occupe par exemple de la traque du commerce de cigarettes illégales et de la criminalité liée à la drogue. Le *Zollkriminalamt* ne mène des enquêtes que sur des infractions particulièrement graves, telles que la prolifération d'armes de destruction massive. Les services d'enquête douanière utilisent le système d'information électronique "*Zollfahndungsinformationssysteme*" (INZOLL), qui est géré par le *Zollkriminalamt*. Les autorités douanières y conservent les dossiers relatifs aux enquêtes douanières dans lesquels figurent des données à caractère personnel. Le BKA a également accès à INZOLL (art. 15 ZFdG 2021).

Le *Zollfahndungsdienst* tombe dans le champ d'application de la *Zollfahndungsdienstgesetz* (ZFdG), modifiée cette année par la *Gesetz zur Neustrukturierung des Zollfahndungsdienstgesetzes*. L'échange de données à caractère personnel avec les États membres de l'UE est régi par l'article 22. Les dispositions relatives à l'échange d'informations au sein de l'Allemagne, telles qu'elles sont définies à l'article 21, alinéas 2 à 11 s'appliquent *mutatis mutandis*. La responsabilité quant à l'admissibilité des transferts de données incombe au *Zollkriminalamt*. Les transferts à un service de police ou à une autre autorité publique d'un État membre de l'UE sur la base d'accords particuliers de droit international restent admissibles (art. 22, al. 1 ZFdG 2021). L'article 24 de la ZFdG contient un certain nombre d'interdictions concernant la communication d'informations et les motifs de refus. En plus des interdictions générales de fournir des informations figurant à l'article premier, le deuxième paragraphe contient un certain nombre de motifs supplémentaires pour refuser de transmettre des informations à un pays étranger.

⁸⁵ Art. 2, al. 2, de la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen, telle que modifiée par la décision-cadre 2009/299/JAI.

3.3.3 Échange international d'informations administratives

En Allemagne, le règlement général sur la protection des données 2016/79/UE a été intégré dans la *Bundesdatenschutzgesetz (loi fédérale sur la protection des données) (BDSG)*. Cette loi permet d'utiliser les données à des fins autres que celles pour lesquelles elles ont été collectées (art. 49 BDSG). Les conditions de nécessité et de proportionnalité s'appliquent. Comme en Belgique, les données peuvent être traitées par les autorités publiques pour la prévention, la détection, la poursuite ou la répression des infractions pénales ou des crimes, dans la mesure où ces autorités traitent les données pour remplir ces tâches. La prévention des infractions comprend également la protection contre les menaces à la sécurité publique et leur prévention (art. 45 BDSG). Si ce qui est indiqué à l'article 45 n'est pas applicable, le traitement à d'autres fins n'est possible que s'il existe une base juridique distincte (art. 49, BDSG).

3.4 Les cadres juridiques nationaux aux Pays-Bas

3.4.1 Échange international d'informations en matière pénale

Le traitement des données à caractère personnel dans le domaine des enquêtes et des procédures pénales est régi aux Pays-Bas par la loi sur les données de police et la loi sur les informations judiciaires et de procédure pénale.⁸⁶ La mise en œuvre de cette législation est précisée dans le décret sur les données de police et le décret sur les données judiciaires et de procédure pénale, respectivement. Compte tenu du champ d'application de ce précis, la réglementation générale sur l'assistance juridique dans le Code de procédure pénale ne sera pas abordée⁸⁷, étant donné que cette réglementation ne concerne essentiellement que l'assistance juridique aux pays hors de l'UE.⁸⁸

Le Centre (national) international d'entraide judiciaire

Aux Pays-Bas, toutes les demandes d'entraide policières et judiciaires internationale, qu'elles soient entrantes ou sortantes, sont traitées par le réseau des Centres d'Entraide Judiciaire Internationale (CEJI). Un CEJI est un partenariat entre le Ministère public et la police. Chaque parquet d'arrondissement et unité de la Police Nationale dispose d'un CEJI, le Centre National d'Entraide Judiciaire Internationale (CNEJI) étant rattaché au Parquet national et à la Police nationale. Le CNEJI traite les demandes d'entraide judiciaire en relation avec le Bureau du Procureur national. Le LIRC sert également de point de contact international pour les autorités étrangères dans les cas où une demande d'entraide policière ou judiciaire n'est pas directement adressée à un CEJI régional, coordonne le traitement des demandes qui nécessitent l'intervention de plusieurs CEJI et traite les demandes qui ne peuvent être rattachées à un CEJI.⁸⁹ Le CNEJI gère également les cinq canaux d'échange d'informations policières internationales, à savoir INTERPOL, Europol, SIRENE, les agents de liaison étrangers accrédités pour les Pays-Bas et les agents de liaison néerlandais en poste à l'étranger.⁹⁰ Le CNEJI est également le centre international d'entraide judiciaire pour la Police nationale, la Maréchaussée Royale néerlandaise et les services spéciaux d'investigation.⁹¹ Les C(N)EJI utilisent actuellement encore le système national d'enregistrement uniforme pour l'entraide judiciaire internationale (LURIS pour *Landelijk Uniform Registratiesysteem*), qui enregistre toutes les demandes d'entraide judiciaire entrantes et sortantes.⁹² Il est toutefois prévu que ce système soit remplacé à l'avenir par le système néerlandais d'assistance internationale (DIAS pour *Dutch International Assistance System*).⁹³

86 I. Helsloot et al (2013). *Evaluatie Wet justitiële en strafvorderlijke gegevens*, Boom Lemma Publishers, p. 56.

87 Compris dans les articles 5.1.1. à 5.1.13. du Code de procédure pénale.

88 *Documents parlementaires II*, session 2015/16, 34 493, n° 3, p. 3 ; P.A.M. Verrest, Remarques introductives à : *Wetboek van Strafvordering, Eerste afdeling verzoek voor internationale rechtspulp in strafzaken*, in C. Cleiren, J. Crijns & M. Verpalen (2021, éd.). *Tekst & Commentaar Strafvordering*. Wolters Kluwer.

89 Annexe aux *Documents parlementaires I*, session 2018/19, 30 880 ; *Documents parlementaires II*, session 2016 /17, 27 925, n° 613, p. 1.

90 *Documents parlementaires II*, session 2016/17, 27925, n° 613, p. 1.

91 Police nationale, *Inrichtingsplan Nationale Politie*, La Haye : Ministère de la Justice et de la Sécurité 2012 (version 3.0), p. 194.

92 Conseil de l'Union européenne 3 février 2014, 13681/2/13 REV 2, p. 8.

93 New 'Dutch International Assistance System' ", justid.nl, 22 avril 2020.

Loi sur les données de police

Sur la base de la Décision-cadre suédoise, l'UE dispose de son propre régime de divulgation pour l'échange de données policières, qui a été mis en œuvre dans la loi sur les données policières (*Wet Politiegegevens*, ci-après dénommée Wpg) et l'arrêté d'exécution sur les données policières (*Besluit politiegegevens*, ci-après dénommé Bpg). La Wpg est entrée en vigueur en 2008 et a été modifiée pour la dernière fois en 2019 dans le cadre de la mise en œuvre de la directive sur la protection des données en matière d'enquêtes et de poursuites.⁹⁴ La loi vise à assurer un équilibre entre une bonne application de la loi d'une part et les intérêts de la vie privée des citoyens d'autre part.⁹⁵ La Wpg ne concerne que le traitement des données de police, qui sont définies comme des données traitées en tant que données à caractère personnel dans le cadre de l'exécution de la mission de police, telle que visée à l'article 3 (maintien effectif de l'ordre public et octroi d'assistance) et à l'article 4 (missions confiées à la Maréchaussée royale néerlandaise) de la loi sur la police de 2012 (art. 1, sub. a, Wpg). Les fonctions de police comprennent également les fonctions au service de la justice, telles que décrites à l'art. 1 alinéa 1 sous i de la loi sur la police de 2012.⁹⁶

Le champ d'application de la Wpg a été réduit par la mise en œuvre de la directive (UE) 2016/680 sur la protection des données pour la recherche et la poursuite d'infractions pénales, qui concerne le traitement des données à caractère personnel dans le cadre de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ou de l'exécution de sanctions pénales. Cela signifie que lorsque des données à caractère personnel sont traitées dans le cadre de l'exécution de tâches au service de la justice, le RGPD s'applique, étant donné que ces tâches ne concernent pas la recherche et la poursuite d'infractions pénales. Il s'agit par exemple du traitement des données dans le cadre de la loi sur les armes et les munitions et de la loi sur les étrangers de 2000.⁹⁷ Toutefois, la Wpg prévoit une exception pour la loi sur le code de la route (application administrative) en raison de son lien étroit avec l'enquête et la poursuite d'infractions pénales (article 1, sub a de la Wpg).⁹⁸

Il doit également s'agir de traitement des données de police qui ont été versées dans un fichier par une autorité compétente ou qui sont destinées à être versées dans un fichier. Cela signifie que le traitement des données à caractère personnel entre (partiellement) dans le champ d'application de la Wpg lorsqu'il est effectué par la Police nationale, le Service national d'enquête criminelle, la Maréchaussée royale des Pays-Bas et les services d'enquête spéciaux. Depuis l'entrée en vigueur de la directive sur la protection des données pour la recherche et la poursuite d'infractions pénales, la Wpg s'applique également (partiellement) au traitement des données par les agents spéciaux d'investigation.⁹⁹

La transmission d'informations policières à d'autres États membres de l'UE est réglementée par l'article 15a de la Wpg et précisée dans le Bpg. Les conditions générales de la transmission d'informations policières aux Pays-Bas, telles que déterminées à l'article 15 Wpg, s'appliquent *mutatis mutandis* à la transmission de données à d'autres États membres de l'UE.

94 La LPG a été modifiée par l'arrêté du 6 décembre 2018 visant à modifier le décret sur les données de police, le décret sur les casiers judiciaires et criminels et le décret sur les données de police (services spéciaux d'enquête) afin de mettre en œuvre la réglementation européenne sur le traitement des données à caractère personnel à des fins de prévention, d'enquête, de détection et de poursuite des infractions pénales ou d'exécution des sanctions pénales (directive d'application sur la protection des données à des fins d'enquête et de poursuite) (*Bulletin des lois et décrets* 2018, 496). Ce décret est entré en vigueur le 1er janvier 2019.

95 *Documents parlementaires II*, session 2005/06, 30 327, n° 3, pp. 1-2.

96 Selon l'article 1er, section i, de la loi de 2012 sur la police, on entend par « missions de police au service de la justice : 1° l'exécution des règlements légaux dont Notre ministre est chargé ainsi que l'exécution des règlements légaux fixés dans ou en vertu de la loi de 2000 sur les étrangers ; 2° le règlement de droit administratif des infractions aux règlements légaux, dans la mesure où ces règlements ont confié le contrôle de l'exécution des missions de police au ministère public ; 3° la signification des avis judiciaires dans les affaires pénales, le transport des personnes privées de liberté par la loi et le service de la justice ». »

97 *Documents parlementaires II*, session 2017/18, 34 889, n° 3, p. 12.

98 *Documents parlementaires II*, session 2017/18, 34889, n° 3, p. 12.

99 Arrêté du 6 février 2019, *Stb.* 2019, 85, p. 5 ; Les Pays-Bas comptent 4 services spéciaux d'investigation, à savoir le Service de renseignements et d'enquête fiscaux (à savoir le *Fiscale Inlichtingen- en Opsporingsdienst* ou FIOD), l'Inspection des affaires sociales et de l'emploi, Direction des enquêtes, (à savoir de *Inspectie Sociale Zaken en Werkgelegenheid*, *Directie Opsporing*, ou ISZW-DO), l'Autorité néerlandaise de sécurité des aliments et des produits de consommation, Service de renseignement et d'enquête (à savoir de *Nederlandse Voedsel- en Warenautoriteit, Inlichtingen- en Opsporingsdienst* (NVWA-IOD), et l'Inspection de l'environnement et des transports, Service de renseignement et d'enquête (à savoir de *Inspectie Leefomgeving en Transport, Inlichtingen- en Opsporingsdienst* ou ILT-IOD).

La Décision-cadre identifie le « service répressif compétent » comme l'autorité ayant le pouvoir de fournir des informations, pour lequel la définition suivante est donnée à l'article 2 sub.a de la Décision-cadre : « une autorité nationale, policière, douanière ou autre habilitée par le droit national à détecter, prévenir ou enquêter sur des infractions ou des activités criminelles et à exercer son autorité et prendre des mesures coercitives dans le cadre de ces activités ». Aux Pays-Bas, le service national d'organisation de l'information (*Dienst Landelijke Informatie Organisatie*, ci-après dénommé DLIO), qui fait partie de l'unité nationale de la police néerlandaise, joue le rôle de l'autorité répressive compétente.¹⁰⁰ Au sein du DLIO, toutes les activités relatives à l'échange international d'informations sont incluses dans l'éventail des tâches du LIRC.¹⁰¹

L'Arrêté sur les données de police

Le Bpg est l'arrêté général d'exécution de la Wpg et, au paragraphe 5a, il fixe des règles supplémentaires concernant la transmission et la réception d'informations policières à destination ou en provenance d'autres États membres de l'UE. En vertu de l'article 5:3, alinéa 1, du Bpg, les données de police doivent être transmises aux autres États membres de l'UE au profit des personnes ou organes chargés de la prévention et de la recherche des infractions pénales dans l'État membre en question, dans la mesure où ces données sont nécessaires au bon accomplissement de cette mission de police. L'utilisation d'informations comme preuves dans une affaire pénale ne répond pas à cette condition. Ces informations doivent dès lors être obtenues au moyen d'une demande d'entraide judiciaire.¹⁰² En outre, la transmission doit avoir lieu de la même manière qu'une transmission au niveau national. Les exigences imposées aux autorités compétentes des autres États membres ne pourraient donc pas être plus strictes que celles imposées aux policiers néerlandais. En ne faisant pas de la demande préalable une exigence, le législateur a créé la possibilité d'une transmission spontanée d'informations.¹⁰³ Il s'agit de la situation dans laquelle des informations sont transmises à un autre État membre de sa propre initiative sans qu'une demande d'entraide judiciaire n'ait été introduite.¹⁰⁴ Si les données de police sont reçues spontanément, l'autorité destinataire aux Pays-Bas doit immédiatement évaluer si les données concernées sont nécessaires à la finalité poursuivie et veiller à ce que les restrictions éventuelles au traitement soient respectées.¹⁰⁵

Le principe de base est la transmission, sauf si l'un des motifs mentionnés au deuxième alinéa de l'art. 5:3 Bpg s'applique. Dans ce cas, la transmission peut être refusée ou assortie de conditions restrictives. Les motifs généraux de refus de l'article 2:13 Bpg s'appliquent *mutatis mutandis* à la transmission de données à d'autres États membres (art. 5:3 al. 2 sous a Bpg). Par exemple, les données concernant les informateurs et les données qui peuvent constituer un danger pour les personnes impliquées ou les tiers ont été incluses comme motifs généraux de refus de transmission d'informations policières. En outre, l'article 5:3 alinéa 2 Bpg mentionne un certain nombre de motifs spéciaux de refus pour la transmission de données aux États membres de l'UE. Les transmissions peuvent être refusées ou soumises à des conditions restrictives si la transmission porte atteinte aux intérêts essentiels de la sécurité nationale ; au succès d'une enquête ou d'un traitement en cours (tel que visé à l'art. 10, al.1, sub.a) ou la sécurité des personnes ; est disproportionnée ou même non pertinente par rapport à la finalité pour laquelle elle a été demandée ; concerne une infraction punie aux Pays-Bas d'une peine maximale d'un an d'emprisonnement ; requiert le consentement d'un membre du Ministère public mais celui-ci n'a pas été donné, ou ; concerne des données de police fournies par un autre pays qui n'a pas donné son consentement à la transmission des données par le pays qui les a reçues. Un exemple de motif de refus lié à l'absence de consentement d'un membre du Ministère public (voir sub.f) est une demande d'informations pour laquelle il est nécessaire de recourir à des mesures coercitives ou à des pouvoirs d'enquête spéciaux afin de la traiter. Une telle demande ne peut être traitée indépendamment par la police, car elle relève de l'autorité du procureur général.¹⁰⁶ Même si l'autre État membre souhaite utiliser les informations comme preuve, une

¹⁰⁰ M. Mol Lous & K. van Horssen (2021). Commentary on art. 5:3 Bpolg. in P. Verrest & J. Ouwkerk (ed.), *Tekst & Commentaar Internationaal Strafrecht*, Wolters Kluwer .

¹⁰¹ *Documents parlementaires II*, session 2016/17, 27925, n° 613, p. 1.

¹⁰² Instructions sur l'échange d'informations dans le cadre de l'entraide judiciaire en matière pénale (552i Sv.), paragraphe 4.2.

¹⁰³ Décret du 14 décembre 2007 portant des dispositions d'exécution de la loi sur les données policières (*Stb.* 2007, 550), p. 89.

¹⁰⁴ Décret du 14 décembre 2007, portant des dispositions d'exécution de la loi sur les données de police (*Stb.* 2007, 550), p. 88 ; voir l'article 7 de la Décision-cadre 2006/960/JAI ; selon la Décision-cadre suédoise, l'échange spontané de données devrait en tout cas avoir lieu lorsqu'"il existe des raisons factuelles de croire que ces informations et renseignements pourraient contribuer à la détection, à la prévention ou à l'investigation des infractions définies à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI" (art. 7, al. 1).

¹⁰⁵ L'art. 5:3 alinéa 8 Bpg stipule que l'art. 5:2 ADP s'applique *mutatis mutandis*.

¹⁰⁶ Voir l'article 5.1.7. Code de procédure pénale et la directive de politique criminelle relative à l'échange d'informations dans le cadre de l'assistance mutuelle en matière pénale (552i Code de procédure pénale.), art. 3.2.

demande doit être soumise aux autorités judiciaires.¹⁰⁷

La transmission des données s'effectue à la condition que les données ne soient traitées que dans le but pour lequel elles ont été transmises (Art. 5:3, al. 4 Bpg) et que les données soient détruites dès que les finalités prévues ont été atteintes (Art. 5:3, al. 5 Bpg). L'autorité néerlandaise peut, si la loi l'exige, imposer à l'autorité destinataire des délais au terme desquels les données transmises doivent être détruites (art. 5:3, par. 6 Bpg). Les délais de traitement des données policières spécifiques tels que décrits dans la Wpg sont des exemples de ces délais découlant de la loi.

Le neuvième alinéa de l'art. 5:3 Bpg est d'une grande pertinence pour ce précis. Cet alinéa prévoit que la transmission d'information vers une zone frontalière aux fins de la répression pénale ou du maintien de l'ordre public peut avoir lieu sans l'intervention de l'Unité nationale (*Landelijke Eenheid*)¹⁰⁸ si cela résulte d'un traité auquel la Belgique ou l'Allemagne sont également parties contractantes ou si cela résulte d'une décision sur la base du Traité sur le fonctionnement de l'Union européenne. Les conventions de Senningen et d'Enschede sont particulièrement pertinentes à cet égard¹⁰⁹. Un règlement analogue concerne le maintien de l'ordre et de la sécurité publics ou la prévention des infractions pénales (art. 20 de la convention d'Enschede). Le neuvième alinéa de l'art. 5:3 Bpg stipule en outre que si l'intervention de l'Unité nationale n'est pas requise (comme décrit ci-dessus), les motifs de refus du deuxième alinéa ne s'appliquent pas aux transmissions dans les zones frontalières.

En cas de réception de données policières en provenance d'un autre État membre de l'UE, l'autorité néerlandaise compétente contrôle le respect des conditions imposées par l'État membre expéditeur en vertu de l'article 5:4 Bpg. En ce qui concerne les données dactyloscopiques (empreintes digitales et palmaires), l'article 5:5 Bpg permet une transmission automatisée directe vers un autre État membre de l'UE. Les États membres peuvent effectuer une recherche automatisée dans le système automatique d'empreintes digitales des Pays-Bas (à savoir *het Automatisch Vingerafdrukken Systeem Nederlandse Kollektie* ou HAVANK) en comparant les données dactyloscopiques.¹¹⁰ En cas de concordance positive des données, conformément au troisième alinéa, seules les données qui concordent seront transmises sur la base du principe « hit-no-hit ». En outre, il est possible, en vertu de l'article 5:6 Bpg, de fournir des données à une équipe commune d'enquête au sein de l'UE. Une « équipe commune d'enquête » est formée par deux ou plusieurs États membres avec un objectif commun d'enquête. La réglementation européenne en la matière a été transposée en droit néerlandais dans les articles 5.2.1 à 5.2.5 inclus du Code de procédure pénale. La transmission de données policières à une équipe commune d'enquête n'est possible que si les données sont nécessaires pour atteindre les objectifs pour lesquels l'équipe d'enquête a été créée.

Loi sur les informations judiciaires et de procédure pénale

La Loi sur les informations judiciaires et de procédure pénale (*Wet justitiële en strafvorderlijke gegevens* ci-après dénommée Wjsg) est entrée en vigueur en 2004 et, avec la Wpg, a été modifiée pour la dernière fois en 2019 dans le cadre de la transposition de la directive sur la protection des données en matière d'enquêtes et de poursuites.¹¹¹ La Wjsg régit le traitement des données judiciaires¹¹², des données relatives à la procédure pénale, des rapports inclus dans les dossiers personnels, des données d'exécution et des données pénales judiciaires aux Pays-Bas. Pour ces cinq catégories de données, on trouve des régimes différents dans la loi. L'article 16 de la Wjsg constitue la base de la mise à disposition des données judiciaires aux autorités compétentes des autres États membres de l'UE. Ces données doivent être mises à disposition aux fins de la justice pénale (art. 16, al. 1 Wjsg) et il n'est pas permis d'imposer des conditions qui s'écartent de celles qui s'appliqueraient à un transfert comparable de données de police à l'intérieur des Pays-Bas (art. 16, al. 2 Wjsg).

¹⁰⁷ Directive de politique criminelle relative à l'échange d'informations dans le cadre de l'assistance mutuelle en matière pénale (552i Sv.), art. 1. 4.2.

¹⁰⁸ Au sens de l'article 25, paragraphe 1, alinéa b, de la loi sur la police de 2012.

¹⁰⁹ Voir l'arrêté relatif à la mise en œuvre de la directive sur la protection des données (*Stb.* 2018, 496), p. 28.

¹¹⁰ Team Dactyloscopy", politie.nl, consulté le 30 septembre 2021.

¹¹¹ Loi du 17 octobre 2018 modifiant la loi sur les données de police et la loi sur le casier judiciaire et criminel afin de mettre en œuvre la législation européenne relative au traitement des données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales ou d'exécution de sanctions pénales (*Stb.* 2018, 401). Cette loi est entrée en vigueur en 2019.

¹¹² Les données judiciaires sont des données personnelles ou des données relatives à une personne morale concernant l'application du droit pénal ou de la procédure pénale, qui ont été ou sont traitées dans une base de données (art. 1 sous a Wjsg). Voir les articles 6 et 7 de la Wjsg pour une liste exhaustive des données qui doivent être considérées comme des données judiciaires.

En vertu de l'article 39a de la Wjsg, le Collège des Procureurs généraux peut mettre à la disposition de l'autorité compétente d'un autre État membre des données relatives à l'enquête pénale. L'article 42a de la Wjsg prévoit la possibilité pour le Ministre de la Sûreté et de la Justice de mettre à disposition des copies des rapports contenus dans un dossier personnel. La disponibilité des données d'exécution et des casiers judiciaires est basée sur les articles 51b et 51f respectivement. En outre, l'article 16 de la Wjsg s'applique *mutatis mutandis* à ces quatre autres catégories de données.

Arrêté sur les informations judiciaires et de procédure pénale

L'arrêté sur les informations judiciaires et de procédure pénale (ou *Besluit justitiële en strafvorderlijke gegevens* ci-après dénommé Bjsjg) est l'arrêté général d'exécution de la Wjsg et il définit, entre autres, des règles plus détaillées pour l'échange de données avec les États membres de l'UE (voir la section 6 du Bjsjg). Aux Pays-Bas, le service d'information judiciaire (Justid), qui fait partie du ministère de la Sûreté et de la Justice, est l'autorité centrale responsable de cet échange d'informations (art. 1, al. c Bjsjg).

Au sein de l'UE, les États membres sont tenus de transmettre immédiatement les données judiciaires concernant une condamnation définitive d'un ressortissant européen à l'autorité centrale de l'État membre dont la personne condamnée est ressortissante (art. 34 Bjsjg).¹¹³ Ces informations sont ensuite conservées dans la documentation judiciaire (art. 37 Bjsjg). En outre, en vertu de l'article 35, al 1 du Bjsjg, un État membre peut, dans l'intérêt d'une procédure pénale, soumettre à Justid une demande de divulgation d'informations judiciaires. Ces informations sont ensuite envoyées à l'autorité centrale de l'État membre requérant. S'il s'agit de données judiciaires relatives à une infraction visée aux articles 240b, 242 à 250 inclus et 273f du Code pénal, ces données peuvent être transmises en vertu du deuxième alinéa dans l'intérêt d'une procédure d'embauche concernant un poste impliquant un contact direct et régulier avec des enfants. Le troisième paragraphe prévoit la possibilité d'un échange de données à d'autres fins. Pour la transmission de données personnelles traitées dans des fichiers personnels, l'article 35 s'applique *mutatis mutandis* (art. 47a Bjsjg).

Les données judiciaires, les données relatives à la procédure pénale, les données d'exécution et les données pénales judiciaires peuvent être transmises en vertu de l'art. 36 du Bjsjg à condition qu'elles ne soient traitées que pour la finalité concernée ou dans les limites fixées par l'État membre transmetteur s'il y a lieu (art. 36, al. 1 Bjsjg). Dès que la finalité pour laquelle les données ont été transmises est atteinte, les données doivent être effacées par l'autorité destinataire (art. 36, al. 4 Bjsjg). Des délais peuvent également être fixés à cet effet si cela découle de la loi, sauf si les données sont encore nécessaires pour une enquête en cours, la poursuite d'infractions ou l'exécution de peines (art. 36, al. 5 Bjsjg). En vertu de l'alinéa 2, les données pénales ne peuvent être transmises qu'avec l'intervention d'un membre du ministère public. S'il s'agit de données relatives à l'exécution, l'intervention des personnes désignées à cette fin par le Ministre de la Sûreté et de la Justice ou par le Collège des Procureurs généraux est requise. La transmission de données judiciaires pénales ne peut avoir lieu que par l'entremise d'une juridiction qui supporte la responsabilité du traitement.¹¹⁴ Pour la transmission de données personnelles traitées dans des dossiers personnels, l'article 36, alinéas 1, 4 et 5 de l'ACJC s'applique *mutatis mutandis* (art. 47a Bjsjg).

Si les Pays-Bas reçoivent d'un autre État membre des données judiciaires, des données relatives à des procédures pénales, des données d'exécution ou des données judiciaires pénales, la responsabilité du respect des conditions fixées par l'État membre expéditeur incombe à l'autorité néerlandaise destinataire (art. 38 Bjsjg). Là aussi, les données reçues ne peuvent être traitées que pour la finalité pour laquelle elles ont été reçues (art. 38, al. 2 Bjsjg) et doivent être détruites dès que la finalité a été atteinte ou que les délais fixés par l'État membre transmetteur ont expiré (art. 38, al. 3 Bjsjg). Pour la transmission de données à caractère personnel traitées dans des dossiers personnels, l'article 38, alinéas 1 à 4 inclus s'applique *mutatis mutandis* (art. 47a Bjsjg).

3.4.2 Échange international d'informations fiscales

La loi sur l'assistance internationale en matière fiscale (LAIF)

Aux Pays-Bas, la loi sur l'assistance internationale en matière fiscale (ci-après dénommée LAIF) constitue le cadre juridique de l'échange international d'informations fiscales. La base de l'échange d'informations réside

¹¹³ Voir également l'article 4, alinéa 2, de la décision-cadre 2009/315/JAI du Conseil du 26 février 2009 relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres (JOUE L 93/23).

¹¹⁴ Il doit s'agir d'une juridiction au sens de l'article 2 de la loi sur l'organisation judiciaire.

dans les conventions fiscales et le droit européen (art. 1, al. 1 LAIF). La LAIF peut porter sur toute forme d'impôt perçu par ou pour le compte d'un État ou des subdivisions territoriales ou administratives d'un État, y compris les collectivités locales (art. 1, al.2 LAIF). Les troisièmes et quatrièmes alinéas de l'article 1er excluent un certain nombre de taxes et de droits spécifiques (européens). La LAIF est entrée en vigueur en 1986, principalement dans le but de mettre en œuvre la directive 2011/16/UE, et a été modifiée pour la dernière fois en 2020. La LAIF fournit un cadre plus large que la directive susmentionnée en ne mentionnant pas de taxes spécifiques et en incluant les taxes perçues par les autorités locales. Les intérêts, pénalités administratives et amendes liés à ces taxes sont également couverts par la LAIF.

Si les autorités fiscales ont besoin d'informations dans le cadre de la fiscalité (néerlandaise), elles peuvent les demander sur la base de la loi générale sur les impôts d'État (art. 47 à 55 de la loi générale sur les impôts, ci-après dénommée LGI). Certaines de ces dispositions concernent les contribuables et d'autres les tiers tels que les entrepreneurs (art. 53 LGI) ou d'autres organes de société (art. 55 LGI). Certains tiers, tels que les banques et les compagnies d'assurance,¹¹⁵ tenus de fournir régulièrement des informations aux autorités fiscales, conformément à la loi sur l'impôt sur le revenu (article 10:8 de la loi sur l'impôt sur le revenu, ci-après dénommée LIR 2001). L'administration fiscale et douanière a également conclu des accords avec de nombreuses parties privées sur la fourniture et l'échange d'informations.¹¹⁶

L'article 5 de la LAIF stipule que, à la demande de l'autorité compétente d'un État requérant, le Ministre communique à cette autorité compétente tout renseignement en sa possession ou obtenu à la suite d'une enquête administrative susceptible d'être pertinent pour l'administration et l'application de la législation interne de l'État requérant concernant la perception des impôts couverts par le champ d'application de l'assistance mutuelle visé à l'article 1 de la LAIF. Les Pays-Bas doivent fournir des informations aux pays étrangers sur demande, à condition que la demande émane d'une autorité compétente. En outre, ces informations doivent être importantes pour la perception des impôts visés par la loi sur l'impôt sur le revenu. Le Ministre peut, en consultation avec une autorité compétente, désigner des cas ou des groupes de cas dans lesquels il fournira des informations sans demande préalable et déterminer les conditions dans lesquelles les informations seront fournies (art. 6 LAIF). L'article 6c prévoit l'échange automatique de données, dans le cadre des CRS. (Article 6 LAIF). L'article 6c concerne la dernière modification de la Directive en 2018 et indique que les informations sur les décisions transfrontalières antérieures ou les accords antérieurs en matière de prix de transfert sont automatiquement fournies à l'autorité compétente de chaque État membre et à la Commission européenne. Ces informations comprennent les données d'identification de la personne concernée, autre qu'une personne physique, et, le cas échéant, du groupe de personnes auquel elle appartient ; et un résumé du contenu de la décision transfrontalière préalable ou de l'accord préalable en matière de prix de transfert, y compris une description générale des activités commerciales ou des transactions ou séries de transactions concernées (art. 6d). Toutefois, ce résumé ne peut conduire à la divulgation d'un secret commercial, industriel ou professionnel, ni à l'atteinte à l'ordre public de l'État néerlandais.

La section 3 de la LAIF fixe les règles concernant la transmission spontanée d'informations. L'article 7 de la LAIF mentionne un certain nombre de situations dans lesquelles cela se produit. Par exemple, si l'on soupçonne qu'une réduction, une exonération, un remboursement ou une remise d'impôt a été indûment accordé dans l'État membre de l'autorité compétente ou qu'un impôt ne sera pas perçu si les informations ne sont pas transmises.

L'article 8 offre la possibilité de procéder à des enquêtes complémentaires afin d'obtenir les informations demandées par l'État membre requérant, généralement sous la forme d'une enquête menée par un tiers auprès d'un contribuable, comme le prévoit l'article 53 de la LGI. Par conséquent, il semble qu'il n'y ait aucune possibilité de mener une enquête auprès de non-assujettis, en l'occurrence des personnes privées.¹¹⁷ En outre, des contrôles simultanés peuvent être effectués aux Pays-Bas et dans l'autre État (art. 8a LGI). La section 4a de la LAIF concerne la fourniture automatique d'informations dans le cadre des CRS.

La LAIF offre la possibilité d'imposer des amendes administratives si le contribuable, l'assujetti, l'institution financière déclarante ou la personne qui doit fournir l'accès à l'information se rend coupable d'une faute intentionnelle ou d'une négligence grave en ne respectant pas, ou en ne respectant pas à temps, pleinement

¹¹⁵ Article 10.8 de la loi sur l'impôt sur le revenu de 2001, lu conjointement avec l'article 22 de l'arrêté d'exécution de l'impôt sur le revenu de 2001.

¹¹⁶ D. van Hout (2019). *Algemene beginselen van een binair bestuur*, La Haye, p. 16.

¹¹⁷ Booi 2018, p. 81.

ou correctement les obligations visées à l'article 8 et à la section 4a et les dispositions basées sur cet article et la section 10g (article 11 LAIF).

En vertu de l'article 14, les Pays-Bas ne sont pas tenus de fournir des informations si : l'ordre public est en jeu ; si l'information n'a pu être obtenue aux Pays-Bas en vertu des dispositions légales ou de la pratique administrative, ni pour les intérêts y afférents ou les pénalités ou amendes administratives qui s'y rapportent ; s'il est plausible que l'autorité compétente n'ait pas d'abord épuisé, dans son propre pays, les possibilités habituelles d'obtenir l'information demandée par elle-même ; lorsqu'il n'y a pas de réciprocité ; si un secret commercial, industriel ou professionnel pourrait être divulgué ; au cas où la communication de renseignements contreviendrait aux principes d'imposition généralement admis ou à d'autres limites fixées par les dispositions applicables du droit international et interrégional. La transmission d'informations ne peut pas être refusée pour la seule raison que : les informations sont détenues par une banque, une autre institution financière, une personne autorisée ou une personne agissant en tant que représentant ou trustee, ou que les informations concernent les intérêts patrimoniaux d'une personne (Art 14, al. 3 LAIF).

Les informations fournies par le Ministre à l'autorité compétente d'un autre État membre pour la mise en œuvre de la Directive 2011/16/UE peuvent, conformément à l'article 17, alinéa 1, également être utilisés par cet autre État membre : pour l'établissement et la perception d'autres impôts et taxes couverts par la Directive 2010/24/UE ; pour l'établissement et la perception de cotisations de sécurité sociale obligatoires ; dans le cadre de procédures judiciaires et administratives potentiellement répressives suite à la violation de la législation fiscale, sans préjudice des règles et dispositions générales régissant les droits des prévenus et des témoins dans de telles procédures. Ce consentement est en tout cas donné si les informations peuvent être utilisées à des fins similaires aux Pays-Bas (art. 17, al. 2). Enfin, il est possible d'autoriser une autorité compétente d'un État, sur demande, à communiquer des informations obtenues des Pays-Bas à une autorité compétente d'un autre État (art. 17, al. 6).

Douanes et accises

Aux Pays-Bas, l'échange dans le cadre des douanes et accises est soumis aux principes du code des douanes de l'UE. Les règles concernant l'assistance mutuelle ont été fixées dans le Manuel des douanes néerlandais (partie 44.00.00). Les principes généraux sont que l'assistance mutuelle n'est utilisée que lorsque les ressources propres sont épuisées. En outre, le principe de réciprocité s'applique. La manière et l'étendue de l'assistance fournie sont régies par la législation ou la pratique administrative du pays requis. L'entraide n'est pas accordée si elle est susceptible de porter atteinte à l'ordre public ou à d'autres intérêts essentiels de l'État requis.¹¹⁸

Pour l'échange d'informations concernant les douanes et les accises, il n'existe pas aux Pays-Bas de législation comparable à la LAIF. Le principe de base est toutefois le respect de la confidentialité et, en général, les principes généraux de bonne administration s'appliquent. L'article 1:1, alinéa 3 de la loi générale sur les douanes stipule que les dispositions de cette loi ou prises en application de celle-ci servent également à l'accomplissement des obligations découlant des accords de droit international relatifs à l'assistance mutuelle en matière administrative en ce qui concerne la circulation des biens et des marchandises. Cela signifie qu'en principe, les mêmes conditions s'appliquent à l'assistance mutuelle internationale qu'aux échanges au niveau national, sauf s'il existe une base juridique dans un traité, comme indiqué au chapitre 2. En l'absence de base spécifique, des principes généraux s'appliquent, tels que la limitation à la finalité et la confidentialité, à l'aune desquels l'échange d'informations est également testé.¹¹⁹

La Convention Naples II fait référence aux dispositions douanières nationales néerlandaises. Celles-ci peuvent être interprétées de manière large : toutes les lois et tous les règlements peuvent y être inclus lorsque les autorités douanières ont une compétence totale ou partielle sur la circulation transfrontalière des marchandises soumises à des interdictions, des restrictions ou des contrôles, ou dans le cas de droits d'accises non harmonisés.¹²⁰ Cela signifie que les douanes ont également des compétences en vertu de la loi sur l'opium ou de la législation sur la sécurité, la santé, l'économie et l'environnement.

¹¹⁸ Booij, 2018, p. 58.

¹¹⁹ Booij, 2018, p. 59.

¹²⁰ Booij, 2018, p. 60.

3.4.3 Échange international d'informations administratives

Comme expliqué ci-dessus, le Règlement 2016/679, connu aux Pays-Bas sous le nom de *Algemene Verordening Gegevensbescherming* ou Règlement général sur la protection des données, est particulièrement important pour l'échange d'informations entre les organes administratifs d'exécution dans la mesure où il n'existe pas de base juridique dans un traité. Toutefois, les États membres disposent d'une certaine marge de manœuvre pour apporter des précisions, ce qui est précisé dans la loi d'application du règlement général sur la protection des données. Les Pays-Bas ont choisi de s'écarter le moins possible du règlement.¹²¹

¹²¹ Documents parlementaires II, session 2017/18, 34 851, n° 3.

4 Échange de données au niveau national

4.1 Introduction

Ce chapitre se concentre sur la question de savoir quelles informations les différentes institutions peuvent communiquer aux autres autorités publiques. Pour la Belgique, l'Allemagne et les Pays-Bas, sont décrits dans ce précis les cadres juridiques relatifs à la police, au ministère public, aux autorités répressives administratives, aux autorités fiscales et, le cas échéant, à d'autres organismes impliqués dans les enquêtes et l'application des lois. Pour les Pays-Bas, nous évoquons également les centres régionaux d'information et d'expertise (à savoir de *Regionale Informatie- en Expertisecentra* ou RIEC), qui ont été créés dans le cadre de l'approche intégrée de la lutte contre la (organisée) et auxquels participent les communes, la police, le ministère public et les services fiscaux. Les possibilités d'échange au sein de la Belgique (section 4.2), de l'Allemagne (section 4.3) et des Pays-Bas (section 4.4) sont décrites successivement.

4.2 Les possibilités d'échange en Belgique

4.2.1 Fourniture d'informations par la police

Les possibilités légales pour la police belge de fournir des informations sont définies dans la loi sur la fonction de police (ci-après dénommée LFP). L'article 44, alinéa 1 de la LFP décrit les conditions générales qui s'appliquent à la communication d'informations. Une distinction est faite entre les tâches qui relèvent respectivement de police administrative et judiciaire. Les premières tâches sont liées au contrôle (circulation routière, navigation, chemins de fer et aéroports) et au maintien de l'ordre public. Les fonctions de police judiciaire concernent les enquêtes (fédérales) et les fonctions générales de police locale. L'échange d'informations entre les polices est réglementé par la LPC (art. 44/1, al. 2 et 3 LFP).

Lorsque des données à caractère personnel sont collectées et traitées, elles doivent - au regard des finalités de la police administrative et judiciaire - être adéquates, pertinentes et non excessives. La collecte et le traitement doivent être limités à ce qui est nécessaire pour prévenir une menace spécifique ou pour réprimer une infraction pénale spécifique. Les lignes directrices transmises par les autorités administratives ou judiciaires sont également importantes à cet égard. Les données personnelles et les informations contenues dans les bases de données doivent être directement liées à la finalité du traitement. Lors du traitement de données à caractère personnel, il convient de respecter les exigences du RGPD et de la loi du 30 juillet 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (article 44/3, al. 1 LFP).

Les services de police exécutent leurs tâches conformément aux ordres, instructions, revendications et directives des autorités compétentes (art. 5/6 LFP). Pour chaque arrondissement judiciaire, une concertation d'enquête est organisée entre le directeur-coordonateur administratif ou son délégué, le directeur judiciaire ou son délégué, les représentants des services de police locaux et le procureur du Roi, sous la direction de ce dernier. Cette concertation porte principalement sur la coordination des missions de police judiciaire et l'organisation de l'échange d'informations (art. 9 LFP). L'information est également échangée avec le procureur du Roi sous la forme d'un procès-verbal, ou si l'information n'est pas suffisamment concrète, ou s'il y a des doutes quant à son exactitude, sous la forme d'un rapport d'information judiciaire. Si l'information est importante pour l'exercice des fonctions de la police administrative, un rapport d'information administrative est établi.¹²² Les informations sont transmises aux autorités fiscales par l'intermédiaire du ministère public (voir ci-dessous).

La police administrative et les services de police s'informent mutuellement de l'ordre public lorsqu'il y a lieu de prendre des mesures préventives ou répressives. Les services de police informent également les autorités administratives intéressées des événements extraordinaires concernant l'ordre public dont elles ont connaissance (art. 5/2, al. 1, LFP). Le chef de corps de la police locale, le directeur coordonnateur administratif et le directeur judiciaire de la police fédérale informent le bourgmestre sans délai des faits importants qui sont de nature à troubler la tranquillité, la sécurité ou la salubrité publique dans sa commune (art. 5/2, al. 2 LFP). Le chef de corps de la police locale lui fait rapport sur les problèmes de sécurité dans la commune, sur la réalisation des missions de police administrative sur le territoire de la commune et sur l'exécution passée et

¹²² Van Daele & Bollens, 2019.

prévisible du plan zonal de sécurité (article 5/2, al. 3 LFP). Le directeur coordonnateur administratif informe le bourgmestre préalablement de toutes les initiatives qu'il compte prendre dans le cadre de ses compétences sur le territoire de la commune, et qui ont une influence sur la politique communale de sécurité. Il lui fait en outre rapport sur la réalisation des missions de police administrative dont il assume la coordination et qui concernent le territoire de sa commune (art. 5/2, al. 5 LFP). Le chef de corps de la police locale l'informe en outre préalablement des initiatives que la police locale compte prendre sur le territoire de la commune et qui ont une influence sur la politique communale de sécurité (art. 5/2, al. 4 LFP). Les informations fournies par la police administrative au bourgmestre ne peuvent être utilisées que dans le cadre du maintien de l'ordre public. Le bourgmestre ne peut pas diffuser l'information, mais il peut la transmettre à ses collaborateurs directs.

Si, dans le cadre de l'exercice de leurs fonctions de police judiciaire, les services de police prennent connaissance de données à caractère personnel et d'informations pertinentes pour l'exercice de la fonction de police administrative, ces informations sont partagées. Aucune copie des rapports officiels n'est transmise aux autorités répressives administratives, mais les informations pertinentes sont transmises dans des rapports quotidiens, des avis consultatifs ou des rapports d'information administrative.¹²³ L'obligation d'informer ne s'applique pas si la transmission d'information peut porter atteinte à l'exercice de l'action publique. En outre, peuvent être prises toutes les mesures nécessaires à la protection des personnes et de la sécurité ou de la santé publique en cas de péril grave et immédiat pour celle-ci (art. 44/1, al. 4 LFP).

En cas de doute, les services de police consulteront le magistrat compétent et, moyennant l'accord de ce dernier, les informations judiciaires pourront être communiquées au bourgmestre.¹²⁴ Lorsqu'il n'y a pas de lien avec le maintien de l'ordre public, il n'existe aucune base juridique permettant à la police de mettre des informations à la disposition des autorités répressives administratives. Cela signifie que ces informations ne peuvent être fournies dans le cadre d'une approche administrative de la criminalité, sauf avec l'accord du ministère public.¹²⁵

4.2.2 Transmission d'informations par le ministère public

Dans cette section, nous examinons la communication d'informations par le ministère public aux autorités fiscales et aux autorités répressives administratives.

Tout d'abord, le code d'instruction criminelle (ci-après dénommé CIC) permet au procureur du Roi, si une enquête pénale a mis en évidence des indices de fraude en matière d'impôts directs ou indirects, d'en informer le Ministre des Finances ou le service qu'il désigne, d'accorder l'accès au dossier et d'en prendre copie, sauf si l'accès au dossier et la prise de copie peuvent compromettre les enquêtes pénales en cours. Lorsque l'administration fiscale perçoit des impôts, y compris des centimes et des décimes additionnels, des majorations, des amendes administratives et fiscales, pour ces infractions, cela n'entrave pas la procédure pénale, à condition que le traitement fiscal et pénal des faits fasse partie d'un ensemble cohérent dans le temps et dans le contenu (art. 29bis CIC.).

En ce qui concerne l'échange de données pénales avec les autorités répressives administratives, le ministère public peut accorder l'accès aux informations d'un dossier pénal. Toute personne qui n'est pas directement concernée peut demander au ministère public de consulter le dossier pénal ou d'en obtenir une copie (art. 21bis, § 1, al. 2 CIC). Cela signifie qu'un bourgmestre peut également soumettre une telle demande, même pour des décisions administratives. Le magistrat du parquet compétent évalue chaque demande et peut refuser l'accès si les nécessités de l'enquête pénale l'exigent, si l'inspection présente un danger pour les personnes ou constitue une atteinte grave à leur vie privée, ou si le demandeur ne fournit pas de motifs légitimes pour consulter le dossier.¹²⁶ Afin de protéger la vie privée des tiers mentionnés dans le dossier, les documents doivent être anonymisés à cet égard. Il est également possible qu'un rapport soit établi en ne contenant que les informations pertinentes. Les informations fournies peuvent être utilisées pour prendre des décisions administratives.

Le ministère public peut également mettre spontanément certaines données judiciaires à la disposition d'instances administratives, par exemple dans le cadre d'une approche administrative de la criminalité. Cela

¹²³ Van Daele & Bollens, 2019.

¹²⁴ Van Daele & Bollens, 2019.

¹²⁵ Van Daele & Bollens, 2019.

¹²⁶ Van Daele & Bollens, 2019.

vaut non seulement pour les informations de fond, mais aussi pour l'annonce de l'ouverture d'une enquête pénale, de l'engagement de poursuites ou du prononcé d'une condamnation.¹²⁷

4.2.3 Fourniture d'informations par les instances administratives

Pour les instances administratives en Belgique, le RGPD est à nouveau le cadre le plus important, puisqu'il n'existe pas de réglementation spécifique. Les (im)possibilités qu'implique le RGPD ont déjà été abordées dans la section 2.4.1. Les restrictions qui s'appliquent à l'échange international d'informations sont les mêmes que celles qui s'appliquent aux échanges entre autorités locales en Belgique.

Theunis et al. ont souligné la possibilité pour les autorités locales d'obtenir des informations les unes des autres en invoquant la réglementation sur la transparence de l'administration, dans le contexte des infractions environnementales.¹²⁸ La faisabilité pratique de cet échange de données est toutefois déterminée par la rapidité avec laquelle les documents sont mis à disposition et par la nécessité d'anonymiser les données personnelles sur la base du RGPD.

4.2.4 Transmission d'informations par les autorités fiscales

Comme nous l'avons déjà expliqué au chapitre 3, la législation fiscale belge est très restrictive lorsqu'il s'agit de fournir des informations à d'autres autorités. Le Code des impôts sur les revenus 1992 autorise en principe les autres services administratifs de l'État, les parquets et les greffes des tribunaux et de toutes les juridictions, les administrations des communautés, des régions, des provinces, des agglomérations, des fédérations de communes et des communes, ainsi que les institutions ou établissements publics, à fournir les renseignements qui sont nécessaires à ces services, institutions ou établissements pour l'exécution des dispositions légales ou réglementaires qui leur sont confiées (art. 337, al. 2, CIR 92).

Les autorités fiscales peuvent fournir des informations au ministère public dans le cadre d'une procédure fiscale pénale. Selon le Code d'instruction criminelle les faits pénalement punissables aux termes des lois fiscales et des arrêtés pris pour leur exécution ne peuvent être portés à la connaissance du procureur du Roi qu'après autorisation du conseiller général dont les fonctionnaires traitant l'infraction dépendent ou du fonctionnaire assimilé (art 29, §2 CIC)

Cette autorisation est en tout cas donnée lorsqu'il s'agit de fraude fiscale grave, organisée ou non (art. 29, § 3 CIC.). En cas de fraude fiscale dans un contexte de criminalité organisée, une consultation peut être organisée sur la base du code pénal (ci-après dénommé Cp), à laquelle la police participe également (art. 458ter Cp). Le procureur du Roi détermine qui peut participer à la consultation, l'objet de la consultation et les modalités de la consultation. Les participants sont tenus au secret sur les secrets communiqués lors de la consultation, et ceux-ci ne peuvent être utilisés que pour la poursuite pénale des infractions pour lesquelles la consultation a été organisée. (Art. 458ter, § 2 Cp) L'article 337 du CIR 1992 ne s'applique pas aux communes, aux provinces et à l'Agglomération de Bruxelles.¹²⁹ Par conséquent, les fonctionnaires de l'administration des impôts directs ne peuvent pas fournir aux communes des informations fiscales destinées à l'application des règlements communaux. Dans certains cas - comme l'impôt foncier - les communes ont un intérêt à obtenir des informations fiscales et celles-ci peuvent être fournies lorsqu'il s'agit de personnes morales, pour autant que ces informations soient nécessaires à la mise en œuvre des dispositions légales ou réglementaires confiées aux communes et aux provinces (art. 3.19.0.0.2 § 3 du code fiscal flamand). Il n'y a aucune obligation d'accéder à chaque demande. L'administration fiscale flamande doit être la « source authentique » des données. Les autorités locales doivent demander à la source authentique les données qu'elles ont obtenues d'autres autorités. Enfin, le bourgmestre peut, sous certaines conditions, accéder à un dossier fiscal criminel et ainsi obtenir indirectement la connaissance de données fiscales.¹³⁰

4.2.5 Communication d'informations par les autorités douanières

Les possibilités concernant la transmission d'informations par les douanes belges sont déterminées par le code des douanes de l'UE. En outre, des règles sont définies dans la loi générale sur les douanes et les accises

¹²⁷ Van Daele & Bollens, 2019.

¹²⁸ Theunis, Bijmens & Huts, 2020, p. 25.

¹²⁹ Van Daele & Bollens, 2019.

¹³⁰ Van Daele & Bollens, 2019.

(ci-après dénommée LGDA). L'article 320 LGDA précise que les agents des douanes et accises exercent leurs fonctions lorsqu'ils communiquent des informations aux autres services administratifs de l'État, aux administrations des Communautés et des Régions de l'État belge, aux parquets et aux greffes des tribunaux, aux cours de justice et à toutes les autorités judiciaires, ainsi qu'aux institutions ou établissements publics. Les informations sont transmises aux services susmentionnés dans la mesure nécessaire pour assurer l'exécution de leurs tâches légales ou administratives. Cette communication doit se faire conformément aux dispositions des règlements pertinents édictés par l'Union européenne.

Les personnes travaillant dans les services auxquels l'Administration des douanes et accises a fourni des informations de nature fiscale sont tenues au même devoir de confidentialité et ne peuvent utiliser les informations obtenues en dehors du cadre des dispositions légales pour l'exécution desquelles elles ont été fournies. Par « institutions ou établissements publics », on entend les institutions, sociétés, associations, établissements et services à la gestion desquels l'État participe auxquels il accorde une garantie, dont il contrôle les activités ou dont le personnel administratif est nommé par le gouvernement sur sa proposition ou avec son approbation.

4.3 Les possibilités d'échange en Allemagne

4.3.1 Fourniture d'informations par la police

La police allemande se compose de la *Landespolizei*, de *Bundespolizei*, *Bundeskriminalamt* et de la *Polizei beim Deutschen Bundestag*. Ces forces de police utilisent le système électronique commun d'information policière : INPOL-neu. Il s'agit d'un système d'information et d'investigation, composé de dossiers sur des personnes et des affaires, qui est géré par le BKA conformément à l'article 29 du BKAG. Le "*Verbundsystem*" se compose d'*INPOL-Zentral* du BKA et d'*INPOL-Land* (également souvent appelé POLAS ou POLIS) des différents Länder.¹³¹ Les données qui y sont stockées sont accessibles à toutes les autorités connectées. Le BKA, *Bundespolizei* et les autorités policières des Länder, les autorités douanières allemandes ont également accès au système.

Bundeskriminalamt

L'échange de données à caractère personnel en Allemagne par le BKA est réglementé à l'article 25 du BKAG. Cette disposition établit une distinction entre la communication de données par le BKA à d'autres services de police allemands (al. 1), à d'autres autorités et organismes publics (al. 2) et à des organismes non publics (al. 3). Cette section portera uniquement sur les transmissions visées aux alinéas 1 et 2.

Les transmissions aux forces de police allemandes ne peuvent avoir lieu que dans la mesure où cela est nécessaire à l'exécution des tâches du BKA ou du service destinataire. En outre, le BKA peut transmettre des données à caractère personnel à d'autres autorités et à d'autres organismes publics si cela est prévu par d'autres dispositions légales ou si la transmission est nécessaire à l'accomplissement de ses missions ; pour la poursuite des infractions pénales, l'exécution des peines et la procédure de grâce ; à des *fins de Gefahrenabwehr*, ou ; pour prévenir une atteinte grave aux droits d'une personne ou aux fins d'une procédure pénale (art. 25, al. 2 et 3 BKAG).

Les données personnelles reçues ne peuvent en principe être traitées que dans le but pour lequel elles ont été fournies. Le traitement à d'autres fins est autorisé conformément à l'article 12, alinéas 2 à 4 du BKAG, concernant le principe d'une nouvelle collecte hypothétique de données (art. 25, al.6 BKAG). Selon ce principe développé par le *Bundesverfassungsgericht*, le nouveau but doit être la prévention, la détection ou la poursuite d'une infraction au moins aussi grave ou la protection d'un intérêt juridique au moins aussi important, pour lequel un plan d'enquête concret a déjà été établi (art. 12, al.2 BKAG).¹³² Lorsqu'il s'agit du traitement de données obtenues par transmission, la question est en principe de savoir si les données auraient été obtenues pour la nouvelle finalité.

¹³¹ Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht (Version 1.1, juillet 2020), bundesarchiv.de, p. 17.

¹³² Voir également : H. Winter et al (2020), De verwerking van politiegegevens in vijf Europese landen, Pro Facto, p.36.

Le BKA est responsable de l'admissibilité de la transmission. Si la transmission est effectuée sur demande et en vertu de l'article 25, alinéa 1 ou l'article 25, alinéa 2, sub 2 BKAG, l'organisme récepteur en assume la responsabilité. Dans ces cas, le BKA vérifie uniquement si la demande de transmission entre dans le cadre des fonctions du destinataire, à moins qu'il n'existe des raisons particulières d'évaluer l'admissibilité de la transmission (art. 25, al.8 du BKAG).

Les interdictions de divulgation et les motifs de refus sont inclus dans l'article 28 du BKAG. En vertu de cette disposition, la communication d'informations ne doit pas être effectuée si l'intérêt légitime de la personne concernée l'emporte sur l'intérêt général de la fourniture. Une divulgation n'est pas non plus autorisée si elle contrevient aux règles spéciales d'utilisation du droit fédéral. Cette disposition est sans préjudice de l'obligation de respecter les obligations légales de confidentialité ou les obligations de secret imposées par les ordres professionnels ou la fonction publique et qui ne se fondent pas sur des dispositions légales.

Bundespolizei

Les données à caractère personnel peuvent être transmises par la *Bundespolizei*, conformément à l'article 32, alinéa 1 de la BPolG, aux autorités de police dans la mesure où cela est nécessaire à l'exercice des fonctions de police. En outre, il est également possible, en vertu de l'article 2, alinéa 2, de la BPolG, de transmettre ces données aux autorités douanières, si elles accomplissent des tâches liées au contrôle des frontières ou à des poursuites pénales. Ceci s'applique également à l'échange de données personnelles avec la Bundespolizei.

Le deuxième alinéa autorise l'échange de données à caractère personnel avec d'autres organismes publics allemands, dans la mesure où ces données sont nécessaires à l'accomplissement d'une mission confiée à l'organisme en question ; à la prévention d'un danger ; à la prévention d'une atteinte grave aux droits d'une personne ; à la poursuite d'infractions pénales ou administratives et à l'exécution de jugements, et à l'exécution de demandes spéciales conformément à l'article 17, alinéa 2 *Bundesverfassungsschutzgesetzes*.¹³³ Les divulgations aux organismes non publics sont possibles en vertu du quatrième alinéa, mais ne seront pas discutées plus avant.

La *Bundespolizei* est responsable de l'admissibilité de la transmission conformément à l'article 33, alinéa 1 de la BPolG. S'il s'agit d'une transmission sur demande, l'autorité requérante en assume la responsabilité. Dans ce cas, la *Bundespolizei* se contente de vérifier si la demande entre dans le cadre des obligations du destinataire, à moins qu'il n'y ait des raisons particulières de vérifier l'admissibilité de la transmission (art. 33, al.1 BPolG). L'échange de données n'est pas autorisé si les intérêts à protéger de la personne concernée l'emportent sur l'intérêt public de la transmission (art 33, al.3 BPolG). En outre, le destinataire ne peut utiliser les données personnelles transmises que dans le but pour lequel elles ont été transmises. L'utilisation pour une finalité différente est autorisée dans la mesure où les données auraient été fournies pour cette finalité (art. 33, al.6 BPolG).

Police de Rhénanie du Nord - Westphalie

Les différents Länder ont leurs propres lois sur la police. En raison du champ d'application du présent précis, cette section ne portera que sur la législation du Land de Rhénanie du Nord - Westphalie. L'échange d'informations par la police de Rhénanie du Nord - Westphalie en Allemagne est régi par l'article 27 de la PolG NRW. Le premier alinéa stipule que les données à caractère personnel peuvent être échangées entre les services de police dans la mesure nécessaire à l'accomplissement de leurs propres tâches ou de celles du destinataire. Le transfert à une fin autre que celle pour laquelle les données ont été obtenues ou stockées est autorisé dans la mesure où les données auraient également pu être collectées à cette fin, à moins qu'il ne s'agisse de données collectées conformément à l'article 11 de la PolG NRW.¹³⁴

Le deuxième alinéa stipule que le transfert à d'autres autorités et à d'autres organismes publics est possible, dans la mesure où cela est prévu par une autre disposition légale ou dans la mesure où le transfert est

¹³³ L'article 17, alinéa 2, du Bundesverfassungsschutzgesetz concerne les demandes des *Verfassungsschutzbehörden*, des *MilitärischenAbschirmdienstes*, des *Bundesnachrichtendienstes* concernant les informations qui ont été découvertes dans le cadre de l'exercice des fonctions de la police des frontières.

¹³⁴ L'article 11 de la PolG NRW traite de la collecte de données à caractère personnel en vue d'une assistance et d'une action dans des situations dangereuses, par exemple auprès de personnes dont les connaissances ou les capacités sont nécessaires pour prévenir un danger (al. 1).

nécessaire à l'exercice de la fonction de police, à la prévention d'un danger par l'autorité destinataire, à l'exécution d'une autre tâche dans le cadre de la prévention d'un danger par l'autorité destinataire ou à la prévention ou au rétablissement d'une atteinte grave à l'intérêt public ou aux droits d'une personne. La possibilité de transmettre des données personnelles à des personnes ou des services non publics est décrite au troisième alinéa.

L'article 30 de la PolG NRW régit la transmission des données à la police. Selon le premier alinéa, sauf disposition contraire de la loi, les autorités publiques peuvent, de leur propre initiative, fournir des données à caractère personnel à la police si cela s'avère nécessaire pour l'exercice des fonctions de police. Selon le deuxième alinéa, la police peut également adresser une demande aux autorités publiques, pour autant que les conditions de collecte des données soient remplies. L'autorité publique requise contrôle l'admissibilité de la transmission et, ce faisant, vérifie uniquement si la demande relève de la mission de police, à moins qu'il n'existe des raisons de contrôler la légitimité de la demande ou que la loi n'en dispose autrement. L'article 26 de la PolG NRW définit les règles générales de l'échange d'informations, ainsi que certaines interdictions de fournir des informations et les motifs de refus.

4.3.2 Communication d'informations par le ministère public

Informations provenant des dossiers pénaux

Les tribunaux, les *Staatsanwaltschaften* et autres autorités judiciaires ont accès aux dossiers pénaux conformément à l'article 474, alinéa 1, du code de procédure pénale (*Strafprozeßordnung*, ci-après dénommé StPO) si cela est nécessaire dans l'intérêt d'une bonne administration de la justice. Les informations du dossier pénal peuvent également être communiquées à d'autres organismes publics, tels que les autorités administratives, conformément au deuxième alinéa. Cela est possible dans la mesure où les informations sont nécessaires à la constatation, à l'application ou à la protection de procédures relatives à l'infraction. Dans d'autres cas, les données à caractère personnel provenant d'affaires pénales peuvent être transmises d'office à des organismes, tels que des organismes administratifs, sur la base d'une disposition spéciale ou dans la mesure où d'autres données à caractère personnel sont nécessaires à l'accomplissement de la tâche après une transmission d'office. La mise à disposition est également possible si les informations sont nécessaires à la préparation de mesures dont l'entrée en vigueur permet la transmission automatique de données personnelles issues de procédures pénales sur la base d'une disposition spéciale (art. 474, al.2 StPO). Les organismes visés au deuxième alinéa ne sont, en principe, pas autorisés à consulter eux-mêmes les dossiers pénaux, mais reçoivent un résumé des données pertinentes. Toutefois, une exception peut être faite si la transmission de l'information implique un effort disproportionné ou si l'autorité requérante peut démontrer qu'il est nécessaire de pouvoir consulter l'ensemble du dossier pour accomplir ses tâches (art. 474, al.3 StPO). Dans ces conditions, il est également possible d'obtenir l'accès aux preuves saisies (art. 474, al.4 StPO).

Les données à caractère personnel issues de procédures pénales peuvent également être communiquées d'office, en vertu de l'article 477, alinéa 1 du StPO, aux autorités répressives et aux tribunaux aux fins de poursuites pénales et aux autorités et tribunaux compétents en vue de la poursuite d'infractions administratives, si, de l'avis de l'autorité expéditrice ces données sont nécessaires à cette fin (art.477, al. 1 StPO). Une transmission d'office est également autorisée si l'autorité expéditrice estime que la connaissance de ces données est nécessaire, notamment pour l'exécution des peines ou des mesures, 135 l'application des mesures privatives de liberté et des décisions en matière pénale (art. 477, al.2 StPO).

Au cours de la procédure préparatoire et après la clôture définitive de la procédure, le Ministère public décide de fournir ou non des informations et d'accorder l'accès au dossier. Dans tous les autres cas, le président de la juridiction saisie de l'affaire décide. Le Ministère public est également autorisé à divulguer des données personnelles après l'ouverture d'une procédure pénale. Lorsqu'il s'agit de la transmission de données personnelles entre autorités de police ou de l'accès à de tels dossiers, aucune décision du Ministère public ou du président du tribunal compétent n'est requise, à moins qu'il n'y ait des doutes sur leur admissibilité (art. 480 StPO).

Le StPO mentionne à l'article 479 certaines restrictions et interdictions de transmettre des informations. Il est notamment interdit de transmettre des informations, sur demande ou d'office, si cela va à l'encontre du but de

135 Comme indiqué à l'article 11, alinéa 1, 8° *Strafgesetzbuches*.

la procédure pénale, y compris si cela compromet le but de l'enquête dans le cadre d'une autre procédure pénale, ou si des dispositions légales spéciales de la Fédération ou des Länder s'y opposent (art. 479, al.1 StPO).

La transmission automatique de données à caractère personnel du dossier pénal à d'autres organismes publics est régie par des dispositions particulières, conformément à l'article 474, alinéa 2, sub 2, du StPO. La plus importante dans ce contexte est la *Einführungsgesetz zum Gerichtsverfassungsgesetz* (ci-après dénommée EGGVG), qui fixe les règles pour les "*Verfahrensübergreifende Mitteilungen von Amtswegen*" (art. 12 à 22 EGGVG). Le transfert de données à caractère personnel du suspect dans une affaire pénale est autorisé si, du point de vue de l'autorité de transfert, la connaissance des données est nécessaire pour les cas énoncés à l'article 13, alinéa 1, de la EGGVG. Il s'agit, par exemple, d'un cas où une autorité administrative a besoin de données pour prendre une décision concernant une licence ou une autorisation d'exercer une profession et où les données montrent que la personne concernée ne remplit pas ses obligations professionnelles ou émet un doute sur son aptitude ou sa fiabilité (art. 13, al. 1, 5^b EGGVG). En outre, la transmission est autorisée en vertu de l'article 17 de la EGGVG, notamment si la connaissance des données est nécessaire pour poursuivre des infractions pénales ou administratives ou pour prévenir un danger important pour le bien-être ou la sécurité publique (art. 17, al. 1 et 4, EGGVG).

Informations du Registre central fédéral (BZR)

Le *Bundeszentralregister* (BZR) est géré par l'Office fédéral de la justice et comprend, entre autres, des données sur les condamnations pénales et autres décisions de justice dans les affaires pénales. En outre, y sont également enregistrées des décisions administratives qui peuvent être pertinentes du point de vue du droit pénal, comme le retrait de licences ou l'interdiction d'exercer une profession.¹³⁶ Outre son importance pour la justice et la police, le registre peut également intéresser les autorités administratives afin de connaître le passé pénal d'un demandeur de licence ou de subvention, ou des soumissionnaires à des marchés publics.¹³⁷

La BZRG identifie en son article 41, alinéa 1, les autorités qui ont un accès illimité au registre sur demande expresse. Il s'agit des tribunaux, des *Staatsanwaltschaften* et des services d'enquête de la police. L'accès aux inscriptions du registre en vertu de l'article 17 et aux condamnations dans le cadre du système de justice pour mineurs est exclu. Les informations les concernant ne sont communiquées aux tribunaux pénaux et aux *Staatsanwaltschaften* que dans le cadre d'une procédure pénale engagée contre la personne concernée (art. 41, al.2 BZRG). Les autres autorités, y compris les organismes administratifs, n'ont pas accès au BZR, mais peuvent seulement demander un *Führungszeugnis* (certificat de bonne conduite (ci-après dénommé CBC)). Une demande de CBC n'est possible que si elle est nécessaire à l'autorité requérante pour accomplir ses tâches et qu'il n'est pas approprié de demander un CBC à la personne concernée ou qu'une telle demande n'a pas abouti. Si la personne concernée le demande, l'accès au CBC est accordé par l'autorité (art. 31, al. 1 BZRG). Si la protection des mineurs est en jeu, un CBC étendu est envoyé dans les mêmes conditions (art. 31, al.2 BZRG).

4.3.3 Communication d'informations par les organes administratifs

En Allemagne, la *Verwaltungsverfahrensgesetz* (ci-après dénommée : VwVfG) impose généralement aux autorités administratives de s'entraider. Cette section se concentre sur la réglementation applicable en Rhénanie du Nord - Westphalie.¹³⁸ Cette "*Amtshilfe*" implique que chaque autorité fournisse une assistance sur demande. Cette assistance peut être demandée notamment lorsqu'une autorité n'est pas en mesure d'accomplir elle-même l'acte pour des raisons juridiques ou matérielles, par exemple, en raison d'un manque de personnel ou d'équipements nécessaires. L'assistance n'est pas considérée comme nécessaire si l'autorité requise est tenue d'exécuter les ordres de l'autorité requérante ou si les actes font partie de la mission propre de l'autorité requise (art. 4, VwVfG NRW). En outre, une autorité peut demander une assistance si elle n'a pas connaissance de faits qu'elle ne peut recueillir elle-même, ou si elle a besoin de documents ou d'autres preuves qui sont en possession de l'autorité requise. En outre, l'assistance est également possible si une autorité ne peut exécuter la tâche qu'à des coûts sensiblement plus élevés que l'autorité requise (art. 5, VwVfG NRW).

La recevabilité de la mesure mise en œuvre par l'entraide est régie par la loi de l'autorité requérante, tandis que l'exécution est régie par la loi applicable à l'autorité requise. Cela signifie également que l'autorité requérante

¹³⁶ Voir §3 BZRG pour les inscriptions à enregistrer dans le registre.

¹³⁷ T. Spapens, M. Peters & D. van Daele (2015, ed.). *Administrative measures to prevent and tackle crime*. Eleven International Publishing, p. 231.

¹³⁸ *Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen (VwVfG NRW) Bekanntmachung der Neufassung vom 12.11.1999.*

est responsable de la légalité de la mesure à prendre, tandis que la partie requise est responsable de son exécution (art. 7, VwVfG NRW).

Bien que, en principe, l'assistance doit obligatoirement être accordée, il existe également des limites. Tout d'abord, l'autorité requise peut ne pas être en mesure de fournir une assistance pour des raisons juridiques. L'assistance doit également être refusée si elle porte préjudice à la Fédération ou à l'un des Länder. En outre, l'autorité requise n'est pas tenue de transmettre des documents, des dossiers ou des informations si la procédure doit rester confidentielle en raison de sa nature ou de la loi. Il n'y a pas non plus d'obligation d'accorder l'*Amtshilfe* si cela entraîne des coûts disproportionnés pour l'autorité requise, ou si une autre autorité peut accorder la même assistance plus facilement ou à un coût bien moindre. L'assistance peut également être refusée si elle risque d'entraver gravement le travail normal de l'organisme requis. L'autorité requise ne peut refuser l'exécution pour d'autres motifs, tels que son désaccord avec la demande.

4.3.4 Communication d'informations par l'administration fiscale

Les fonctionnaires publics sont tenus au secret en matière fiscale (art. 30, AO). Il s'agit non seulement des informations recueillies dans le cadre de procédures administratives, de procédures d'audit ou de procédures judiciaires en matière fiscale, mais aussi de toute constatation recueillie dans le cadre de procédures pénales pour infraction fiscale ou de procédures d'amendes administratives pour infraction fiscale. Par conséquent, les autorités fiscales ne fournissent pas d'informations aux organismes administratifs. Toutefois, plusieurs exceptions s'appliquent à cette règle générale. Par exemple, les données fiscales peuvent être divulguées dans la mesure où elles servent les objectifs d'une autre procédure administrative, d'audit ou judiciaire en matière fiscale ou d'une procédure pénale pour infraction fiscale. La divulgation d'informations fiscales est également permise dans la mesure où elle est expressément autorisée par la loi ou si les personnes concernées donnent leur consentement. En outre, les informations fiscales peuvent être divulguées s'il existe un intérêt public prépondérant (art. 30, al. 4, OA). Bien que cette notion ne soit pas définie, il est clair qu'elle doit être interprétée de manière restrictive et que la divulgation d'informations fiscales pour ce motif n'est autorisée que dans les cas où il existe un risque de préjudice grave pour l'intérêt public.¹³⁹

En outre, l'article 31a de l'*Abgabenordnung* (AO) autorise la divulgation d'informations fiscales dans le but de lutter contre l'emploi illégal et la fraude aux prestations sociales. La divulgation de la situation de l'intéressé est autorisée par cette disposition dans la mesure où elle est nécessaire à la conduite d'une procédure pénale, d'une procédure relative à une amende administrative ou d'une autre procédure judiciaire ou administrative visant à lutter contre l'emploi ou le travail illégal, à décider de la délivrance ou de la révocation d'une autorisation sur pied de la loi sur l'emploi temporaire ou à décider de l'octroi, de la récupération, du remboursement, du maintien ou de la rétention de prestations de sécurité sociale. En outre, des informations sur la situation de l'intéressé peuvent être fournies dans la mesure où elles sont nécessaires pour demander le remboursement de prestations payées par des fonds publics. Dans tous ces cas, les autorités sont en principe tenues de notifier les faits à l'institution compétente. Cette obligation ne s'applique toutefois pas lorsque cela impliquerait un effort et un temps disproportionnés.

4.3.5 Communication d'informations par le Zollfahndungsdienst

La base de l'échange d'informations par la *Zentralstelle* des autorités douanières, le *Zollkriminalamt*, se trouve au chapitre 3.2 de la *Zollfahndungsdienstgesetz* (ci-après dénommée ZFdG). Pour l'échange de données à caractère personnel en Allemagne, l'article 21 de la ZFdG est particulièrement pertinent. Le *Zollkriminalamt* peut, conformément au premier alinéa, transmettre ces données à d'autres autorités douanières dans la mesure où cela est nécessaire à l'accomplissement de ses propres tâches ou de celles du destinataire (art. 21, al 1 ZFdG 2021). La transmission de données à caractère personnel à d'autres autorités et à d'autres organismes publics n'est autorisée que si elle est prévue par la loi ou si la transmission est permise et nécessaire pour : l'exécution des tâches propres des autorités douanières telles que stipulées dans la ZFdG ; les poursuites pénales; l'application des peines et l'exécution des jugements ou les procédures de grâce ; les finalités du *Gefahrenabwehr*; le respect des demandes d'information d'autres autorités publiques concernant la vérification des antécédents des personnes ; ou la prévention d'un préjudice grave aux droits des personnes et aux fins de la procédure pénale (art. 21, al. 2 ZFdG 2021). Pour la transmission de données à l'Office fédéral de l'Économie et des Exportations (*Bundesamt für Wirtschaft und Ausfuhrkontrolle*), il doit exister des indices concrets que la connaissance des données est nécessaire pour les cas prévus par la disposition, par exemple

¹³⁹ A. Pahlke & U. Koenig (2004). *Abgabenordnung §§1 à 368*. Beck.

dans le cadre d'une procédure d'autorisation (art. 21, al. 3 ZFdG 2021). La transmission aux organismes non publics est réglementée au sixième alinéa, mais ne sera pas abordée plus avant. Les données qui, conformément aux articles 41 et 61 tomberaient dans le champ d'application de la *Bundeszentralregistergesetz* sont soumises aux restrictions spécifiées à l'article 21, alinéa 8 de la ZFdG 2021).

Le *Zollkriminalamt* est responsable de l'admissibilité de la transmission. Si la transmission a lieu sur demande, l'autorité requérante en porte la responsabilité. Dans ce cas, le *Zollkriminalamt* se contente de vérifier si le contenu de la demande de transmission tombe dans le cadre des tâches du destinataire, à moins qu'il n'existe des raisons particulières de vérifier l'admissibilité de la transmission (art. 21, al. 9 ZFdG 2021). En principe, les données à caractère personnel ne peuvent être traitées que dans le but pour lequel elles ont été obtenues. Le traitement à d'autres fins est autorisé, à condition que les données aient également été transmises à cette fin (art. 21, al. 1 ZFdG 2021).

L'article 24 de la ZFdG contient un certain nombre d'interdictions de transmission qui s'appliquent à l'échange national d'informations. Le *Zollkriminalamt* peut ne pas transmettre des données personnelles s'il apparaît clairement que, compte tenu de la nature des données et de leur collecte, les intérêts à protéger l'emportent sur l'intérêt public à la transmission. Cette interdiction ne s'applique pas aux transmissions aux *Staatsanwaltschaften* et aux tribunaux. La communication de données est également interdite si des dispositions particulières du droit fédéral l'empêchent. Les obligations légales de confidentialité ou les obligations spécifiques de secret qui ne sont pas fondées sur une disposition légale ne sont pas affectées.

4.4 Les possibilités d'échange aux Pays-Bas

4.4.1 Échanges au sein des centres régionaux d'information et d'expertise (CRIA)

Après les expériences positives d'une approche intégrée des problèmes complexes de criminalité et de sécurité dans divers endroits des Pays-Bas, les règles de coopération dans ce domaine ont été établies en 2008 dans l'accord administratif sur l'approche décentralisée intégrée de la criminalité organisée.¹⁴⁰ Le système utilisé pour renforcer la coopération entre les silos de droit pénal et administratif est le partage d'informations et la mise en œuvre d'interventions ciblées et adéquates. Onze centres régionaux d'information et d'expertise (*Regionale Informatie- en Expertise Centra*, ci-après dénommés RIEC's) ont été créés pour soutenir ce type de coopération de manière structurelle. L'amélioration de l'échange d'informations entre les services concernés a été identifiée comme une condition préalable importante. En tant que courtiers en informations entre les services traditionnels de répression et d'investigation, d'une part, et les communes et les provinces, d'autre part, les RIEC's ont pour mission d'intensifier l'échange d'informations de manière efficace, efficiente et légale. Les principes généraux de légitimité pour le traitement et l'échange de données à caractère personnel par les organismes participant¹⁴¹ aux RIEC's sont décrits dans la section 6 du protocole de confidentialité des RIEC's-LIEC.¹⁴²

Le règlement général sur la protection des données (RGPD) et la loi d'application du RGPD (*Uitvoeringswet Algemene verordening gegevensbescherming*, ci-après dénommée UAVG) s'appliquent au traitement des données au sein du RIEC. La base du traitement des données par le partenariat se trouve à l'article 6, premier alinéa, sous e, du RGPD. Cette base implique que le traitement des données à caractère personnel n'est licite que si et dans la mesure où le traitement est nécessaire à l'exécution d'une mission d'intérêt général ou à l'exercice de l'autorité publique dont est investi le responsable du traitement.

Les bases juridiques pour la communication de données à caractère personnel par les organismes qui collaborent au sein des RIEC's se trouvent dans les dispositions légales qui s'appliquent à ces organismes. Il peut s'agir d'articles du RGPD et de l'UAVG, mais aussi d'autres lois dans lesquelles figurent des dispositions relatives à la communication de données à caractère personnel.

¹⁴⁰ Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdad [Accord administratif relatif à une approche décentralisée intégrée de la criminalité organisée], annexe aux *Documents parlementaires II* session 2008/09, 29911, n° 27.

¹⁴¹ Les organismes concernés sont le ministère public, la police, la Maréchaussée royale, les douanes, le FIOD, mais aussi l'administration fiscale et douanière, les communes et les provinces, entre autres.

¹⁴² Protocole de confidentialité pour RIEC's-LIEC, avril 2020.

4.4.2 Communication d'informations par la police et la Maréchaussée royale des Pays-Bas

La communication d'informations policières par la police et la Maréchaussée royale néerlandaise (Koninklijke marechaussee, ci-après dénommée Kmar) à des tiers est régie par la troisième section de la loi sur les informations policières (Wpg). Sur la base de l'article 16 Wpg, la police et la Kmar sont autorisées à fournir des données au Ministère public et aux bourgmestres dans la mesure où ils en ont besoin pour - en bref - la détection respectivement des infractions pénales ou le maintien de l'ordre public. L'article 17 de la Wpg fournit une base pour la communication de données aux services de renseignement. L'article 18, alinéa 1, de la Wpg pose les bases de la mise à disposition structurelle de données à des tiers désignés par ou en vertu d'un arrêté. Les détails se trouvent dans la quatrième section de l'arrêté sur les données de police (Bpg). Celui-ci contient une liste exhaustive d'autorités, stipulant les conditions dans lesquelles les données peuvent être partagées avec chacune d'entre elles. La communication d'informations policières dans le cadre d'une RIEC, par exemple, a été précisée au septième alinéa de l'article 4:3 du Bpg. La communication accessoire d'informations policières à des tiers est possible dans des cas particuliers sur la base de l'article 18, alinéa 2, de la Wpg, avec le consentement ou sur instruction du Ministre de la Sécurité et de la Justice, ou sur la base de l'article 19 de la Wpg, cette communication n'étant autorisée que pour les finalités suivantes : la prévention et la détection des infractions pénales, le maintien de l'ordre public, l'assistance à ceux qui en ont besoin ou le contrôle du respect des réglementations. Dans le même but, la communication de données sur pied de l'article 20 de la Wpg est autorisée à des fins de coopération entre les autorités et personnes ou organismes compétents. Pour toutes ces formes de communication de données, la communication de données n'est autorisée qu'en raison d'un intérêt public important, ce qui signifie que la communication des données revêt pour la société une importance plus que commune.¹⁴³ Conformément aux principes de proportionnalité et de subsidiarité, l'intérêt de communiquer des données à des tiers doit l'emporter sur l'intérêt de protéger la vie privée des personnes auxquelles se rapportent les données de police.¹⁴⁴

4.4.3 Communication d'informations par le ministère public

La communication à des tiers de données relatives aux procédures judiciaires par le Ministère public est régie par la deuxième section du titre 2A de la loi sur les informations judiciaires et de procédure pénale (*Wet justitiële en strafvorderlijke gegevens*, ci-après dénommée Wjsg). En vertu de l'article 39e de la Wjsg, le ministère public est autorisé à fournir des données à divers organismes du système de justice pénale, notamment la police, la Maréchaussée royale néerlandaise et les services d'enquête spéciaux, dans la mesure où cela est nécessaire dans l'intérêt d'un intérêt public important.

En vertu de l'article 39f de la Wjsg, le Ministère public peut communiquer les informations de procédure pénale à d'autres personnes ou organismes, mais uniquement dans la mesure où ces données sont non seulement nécessaires à ces personnes ou organismes en raison d'un intérêt public important ou pour la constatation, l'exercice ou la défense d'un droit en justice, mais sont également communiquées sous une forme telle qu'il est raisonnablement impossible de remonter à des personnes autres que la personne concernée. En outre, la communication de données n'est autorisée qu'à certaines fins, notamment la prévention et la détection des infractions pénales, le maintien de l'ordre et de la sécurité et le contrôle du respect de la réglementation.

La Circulaire relative à la loi sur les informations judiciaires et de procédure pénale, une mise en œuvre du titre 2A de la loi, indique dans quels cas, sous quelles conditions et à qui le Ministère public peut fournir des informations à des fins autres que la procédure pénale. Le chapitre III de la Circulaire indique, entre autres, à qui ou à quelles organisations les informations de procédure pénale peuvent être communiquées en vertu de l'article 39f de la Wjsg. En vertu du chapitre 3 sub a. de la Circulaire, les informations de procédure pénale peuvent être fournies aux bourgmestres, entre autres, aux fins de la prévention et de la détection des infractions pénales. Le chapitre 3, sub. b de la Circulaire permet également de communiquer des informations dans le but de maintenir l'ordre et la sécurité. Le chapitre 3, sub. c de la Circulaire autorise la communication des informations de procédure pénale aux organismes administratifs, y compris l'administration fiscale et des douanes et les services spéciaux d'investigation, aux fins de contrôler le respect de la réglementation. Aux fins de la prise d'une décision de droit administratif, les informations de procédure pénale nécessaires à cette fin peuvent être communiquées, conformément au chapitre 3 sub. d. de la Circulaire, à toutes les administrations (locales), dans la mesure où aucune disposition légale particulière ne s'applique. En vertu du chapitre 3, sub. e de la Circulaire, les informations de procédure pénale peuvent être communiquées à diverses

¹⁴³ Documents parlementaires II, session 2005/06, 30 327, 3, p. 74.

¹⁴⁴ Documents parlementaires II, session 2005/06, 30 327, 3, p. 76.

catégories d'employeurs (y compris le gouvernement) afin d'évaluer la nécessité d'imposer une mesure légale ou disciplinaire. Lorsque cela s'avère nécessaire pour fournir une assistance aux victimes et aux autres personnes impliquées dans une infraction pénale, le chapitre 3, sub. f de la Circulaire autorise également la divulgation des informations de procédure pénale aux victimes et aux organismes d'aide aux victimes, tels que Slachtofferhulp Nederland. Enfin, conformément au chapitre 3 sub. g de la Circulaire, les données requises pour un avis du Bureau de promotion des évaluations d'intégrité de l'administration publique concernant une décision gouvernementale dans le cadre d'une transaction immobilière peuvent être fournies à toutes les agences gouvernementales (locales).

Les données judiciaires peuvent être fournies par le Ministère public en vertu de l'article 8a de la Wjsg, dans la mesure où cela est nécessaire au regard d'un intérêt public important, dans les cas où des données à caractère pénal peuvent être fournies. Le Ministère public peut fournir des données d'exécution (données personnelles ou données sur une personne morale concernant l'exécution de décisions de droit pénal, qui sont ou seront traitées dans un fichier ou une autre base de données) à des personnes ou des organismes dans la mesure où cela est nécessaire au regard d'un intérêt public important. Cela ne peut se faire qu'aux fins suivantes : l'exécution d'une décision de droit pénal, la prévention, la détection, l'investigation et la poursuite d'infractions pénales, la médiation de dettes ou la resocialisation de la personne concernée, l'action administrative ou la prise d'une décision de droit administratif ou l'aide aux victimes. En outre, le Ministère public ne peut fournir ces données que dans la mesure où elles sont nécessaires aux personnes ou organismes destinataires en raison d'un intérêt public important ou de la constatation, de l'exercice ou de la défense d'un droit en justice. Les données doivent également être fournies sous une forme permettant d'éviter raisonnablement de remonter à des personnes autres que la personne concernée.

Conformément à l'article 52 de la Wjsg, les destinataires des données sont tenus d'en préserver la confidentialité. Il existe deux exceptions à cette règle : il est stipulé dans la Wjsg ou dans la réglementation adoptée en son exécution que la communication est autorisée, ou l'exécution de la tâche pour laquelle les données ont été communiquées rend nécessaire le partage des données.

4.4.4 Communication d'informations par les Communes et les provinces

La base générale du partage des données personnelles par les communes et les provinces se trouve à l'article 6, premier alinéa du RGPD. Cette base implique que la communication de données à caractère personnel sans le consentement de la personne concernée n'est licite que si et dans la mesure où la communication des données à caractère personnel est nécessaire pour l'exécution d'un contrat auquel la personne concernée est partie ou pour prendre des mesures à la demande de la personne concernée avant la conclusion d'un contrat ; pour satisfaire à une obligation légale incombant à la commune ou à la province ; pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; pour l'accomplissement d'une tâche d'intérêt général ou d'une tâche dans le cadre de l'exercice de l'autorité publique dont est investie la commune ou la province ; pour la protection des intérêts légitimes de la commune ou de la province ou d'un tiers, alors que les intérêts de la personne concernée ne l'emportent pas sur ces intérêts. Cette mise en balance des intérêts n'est pas de mise lorsqu'il s'agit du traitement de données à caractère personnel par une autorité publique dans le cadre de l'exécution de ses missions.

En outre, en vertu de l'article 28, deuxième alinéa de la loi sur la promotion des évaluations d'intégrité par l'administration publique (*Wet bevordering integriteitsbeoordelingen door het openbaar bestuur*, ci-après dénommée loi Bibob), les communes et les provinces peuvent transmettre les informations contenues dans une recommandation Bibob aux membres de l'organe de consultation tripartite entre la commune, le ministère public et la police, dans la mesure où cela est nécessaire pour aider la commune ou la province à justifier une décision à prendre à la suite de la recommandation. En outre, les communes et les provinces peuvent partager ces données avec la police, le Kmar, le Ministère public, l'administration fiscale et des douanes, le FIOD, le SIOD et les partenaires au sein d'un RIEC, dans la mesure où les données sont nécessaires pour soutenir la commune ou la province dans l'application de la loi Bibob.

4.4.5 Communication d'informations par l'administration fiscale

Par exception à l'obligation de confidentialité prévue à l'article 67, alinéa 1, de l'AWR (*Algemene wet inzake rijksbelastingen*), l'administration fiscale ne peut, conformément au deuxième alinéa 2 de cet article, partager les données fiscales avec des tiers que si cela est nécessaire à l'application de la loi fiscale ou à la perception des impôts, s'il existe une obligation légale de faire ou s'il a été déterminé par arrêté ministériel que la

divulgarion est nécessaire à la bonne exécution d'une tâche de droit public d'un organisme administratif. L'article 43c, paragraphe 1, de l'*Uitvoeringsregeling Algemene Wet inzake Rijksbelastingen* (ci-après dénommé *Uitvoeringsregeling AWR*) montre qu'il existe de nombreuses exceptions au devoir de confidentialité. Cela s'applique notamment au partage de données avec la police, le Kmar, le Ministère public, les communes et les provinces, à condition que ces données soient nécessaires à une coopération efficace et efficiente dans le cadre de l'application et du respect intégral des réglementations gouvernementales, pour autant qu'un pacte ait été conclu avec les destinataires. Grâce à l'Accord administratif relatif à l'Approche décentralisée intégrée de la criminalité organisée¹⁴⁵ et au Pacte relatif à l'Approche administrative et intégrée de la criminalité organisée, à la lutte contre les goulets d'étranglement en matière de répression et à la promotion des évaluations d'intégrité¹⁴⁶, cette dernière condition est remplie dans la mesure où les données sont partagées dans le cadre des RIEC's. En outre, le Ministre peut accorder une dérogation au devoir de confidentialité (art. 67, al. 3 AWR). Au demeurant, l'exemption du devoir de confidentialité ne constitue pas encore une obligation de fournir des informations. Néanmoins, l'administration fiscale a conclu de nombreux accords pour l'échange d'informations et il existe diverses dispositions légales exigeant la divulgation d'informations. À l'heure actuelle, il n'est pas possible de déterminer quelles informations fiscales l'administration fiscale et des douanes néerlandaise échange avec d'autres organismes administratifs.¹⁴⁷ L'AVG s'applique au partage des données personnelles par l'administration fiscale et des douanes.

4.4.6 Communication d'informations par les douanes et la DGIF

Douane

Les douanes sont régies par le Code des douanes de l'Union (CDU) et la loi générale sur les douanes (*de Algemene Douanewet*, ci-après dénommée *Adw*). En ce qui concerne le trafic transfrontalier de marchandises, la disposition relative au secret de l'article 12 du CDU s'applique. Par exception, en vertu de l'article 1:33, 3ème alinéa de l'Adw, l'échange de données est possible dans la mesure où les données sont nécessaires à la mise en œuvre d'un règlement figurant à l'annexe de l'Adw et à condition que le requérant soit désigné dans une loi figurant à l'annexe de l'Adw et soit autorisé à effectuer des recherches. L'annexe contient une liste de réglementations nationales (près de 75 actes) dans lesquelles les Douanes, entre autres, se sont vu attribuer des tâches. Ainsi, les Douanes peuvent échanger des données sur les mouvements transfrontaliers de marchandises aux fins de la loi en question avec d'autres autorités de contrôle qui sont également nommées dans ces lois et qui sont chargées des règlements pertinents en vertu de ces lois.

En outre, les douanes sont chargées des tâches découlant de la loi sur les droits d'accises (*Wet op de accijns*, ci-après dénommée *WACC*), qui est liée à l'AWR. Pour l'échange d'informations concernant les droits d'accises nationaux, la base est fournie par l'article 43c, premier alinéa du *Uitvoeringsregeling AWR*. Cette possibilité est identique à celle décrite ci-dessus pour les autorités fiscales. Cette exception à l'obligation de secret concernant les données fiscales, prévue à l'article 67, premier alinéa de l'AWR, s'applique aux Douanes de la même manière qu'à l'administration fiscale. Si les exceptions susmentionnées ne s'appliquent pas, les Douanes peuvent échanger des données avec l'administration fiscale et des douanes conformément à l'article 55 de l'AWR.

Service d'enquête et d'intelligence fiscale (FIOD)

Pour l'échange de données par les services spéciaux d'investigation, y compris le Fiscale Inlichtingen- en Opsporingsdienst (ci-après dénommé *FIOD*, Service d'enquête et d'intelligence fiscale), les mêmes conditions que pour la police s'appliquent (à quelques exceptions près), comme le prévoient la loi sur les données de police et l'arrêté sur les données de police.¹⁴⁸ Le *FIOD*, comme la police, n'est donc autorisé à fournir des informations policières qu'en vue d'un intérêt public important, à condition que l'intérêt à fournir des informations à des tiers l'emporte sur l'intérêt à protéger la vie privée de la personne à laquelle les informations policières se rapportent.¹⁴⁹

¹⁴⁵ Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdad [Accord administratif relatif à une approche décentralisée intégrée de la criminalité organisée], annexe aux *Documents parlementaires II*, session 2008/09, 29911, n° 27.

¹⁴⁶ Pacte sur l'approche administrative et intégrée de la criminalité organisée, lutte contre les goulets d'étranglement en matière d'application de la loi et promotion des évaluations d'intégrité, Landelijk Informatie en Expertise Centrum (LIEC), septembre 2014.

¹⁴⁷ Voir M. Snippe (2019). De integratie van fiscale gegevens in het rijksbrede toezicht. Onderzoek naar een veilige haven voor de fiscale informatierijkdom. Wolters Kluwer, chapitre 6 et annexes d'accompagnement.

¹⁴⁸ Décret sur les données de police (services d'enquêtes spéciales).

¹⁴⁹ *Documents parlementaires II*, session 2005/06, 30327, 3, p. 74-76.

5 Conclusion

En conclusion, il convient de souligner que ce précis a pour but de fournir un aperçu pratique des lois et réglementations les plus importantes concernant l'échange d'informations entre les agences de l'Euregio Meuse-Rhin qui peuvent contribuer à la détection et à la lutte de la criminalité transfrontalière dans la région. Cela ne change rien au fait qu'il existe peut-être d'autres lois et règlements, plus obscurs, qui pourraient constituer des bases légales à l'échange d'informations. Cela s'applique en particulier au partage de données avec des partenaires privés, ainsi qu'à l'utilisation de données accessibles au public, telles que les informations du cadastre ou registre foncier, qui ne font pas l'objet de ce précis. Il va sans dire que le présent précis ne s'attache pas à déterminer comment interpréter exactement les différentes lois et réglementations, ni la jurisprudence existante en la matière. Le précis ne doit donc pas être lu comme un document contenant les solutions aux problèmes pratiques rencontrés par les organisations dans leur pratique quotidienne, mais avant tout comme une source d'information sur les lois et règlements pertinents à prendre en compte dans l'échange transfrontalier d'informations.

Comme le montre ce précis, il existe des différences considérables en matière de possibilités dans les domaines du droit pénal, fiscal et administratif. Dans le premier cas, un large cadre juridique a désormais été établi, tant dans le contexte de l'UE que sur le plan multilatéral et bilatéral. Cela s'applique également à l'échange d'informations fiscales, y compris les informations douanières. Ces cadres internationaux n'existent pratiquement pas pour l'échange de données entre les autorités chargées de l'exécution administrative, et le RGPD en détermine largement les possibilités ou les impossibilités. En outre, les cadres juridiques disponibles sont presque entièrement axés sur l'échange d'informations entre les autorités ayant une mission comparable, tandis que les possibilités de partage de données entre les autorités de droit pénal, fiscal et administratif sont encore souvent limitées, tant au niveau international que national. Des améliorations sont certainement envisageables dans ce domaine, afin de renforcer encore la lutte contre la criminalité (transfrontalière).

Enfin, il est important de souligner que le cadre juridique de l'échange (international) d'informations relatives à la lutte contre la criminalité est en constante évolution. Alors même que ce précis est achevé, de nouveaux traités et de nouvelles législations nationales sont en cours d'élaboration ou sont sur le point d'entrer en vigueur. L'utilisateur de ce précis est donc invité à garder un œil sur ces nouvelles possibilités et à les utiliser dans la mesure du possible.