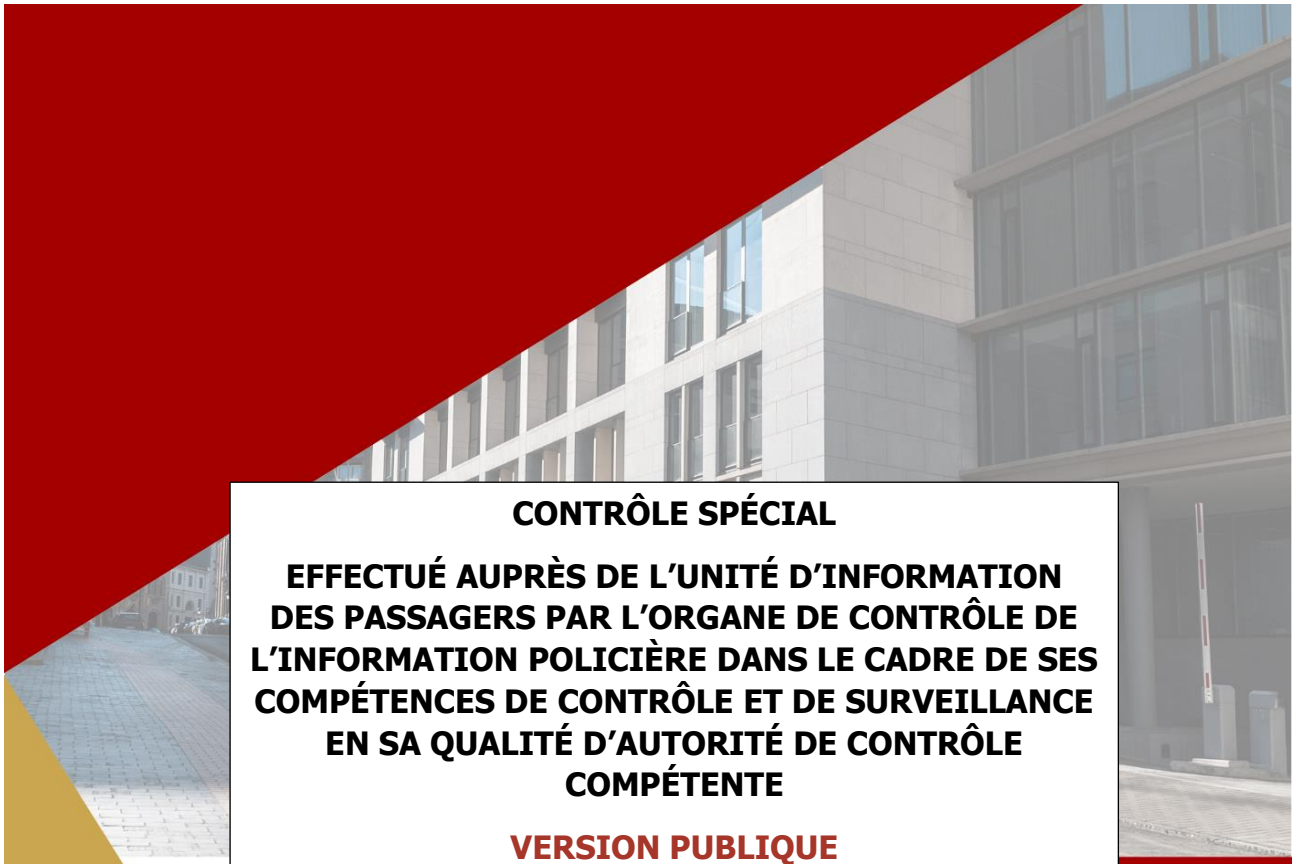

CONTRÔLE SPÉCIAL

EFFECTUÉ AUPRÈS DE L'UNITÉ D'INFORMATION DES PASSAGERS PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SES COMPÉTENCES DE CONTRÔLE ET DE SURVEILLANCE EN SA QUALITÉ D'AUTORITÉ DE CONTRÔLE COMPÉTENTE

VERSION PUBLIQUE

Référence : DAB21001

TABLE DES MATIÈRES

LES COMPÉTENCES DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[1] a réformé l'Organe de contrôle de l'information policière ('Organe de contrôle' ou 'COC') en une autorité de surveillance à part entière en plus des compétences de contrôle en matière de gestion de l'information policière prévues par la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1er et les titres 2 et 7 de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/14 inclus de la LFP, relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de la gestion de l'information et de l'intervention policière. Le COC a dès lors en vertu de la réglementation susmentionnée une compétence générale de surveillance à l'égard de tous les traitements opérationnels et non opérationnels de données (à caractère personnel) par la GPI[2].

L'Organe de contrôle est compétent pour les services de police[3], pour l'inspection générale de la police fédérale et de la police locale (AIG)[4] et pour l'unité d'information des passagers (BEL-PIU)[5]. La compétence de surveillance de l'Organe de contrôle à l'égard des services de police couvre comme nous le disions à la fois les activités de traitement opérationnelles et non opérationnelles[6].

Pour ce qui est de la mission de contrôle, l'Organe de contrôle est chargé du contrôle du traitement des informations et des données visées à l'article 44/1 de la LFP, y compris celles introduites dans les banques de données visées à l'article 44/2, ainsi que de toute autre mission qui lui est confiée par ou en vertu d'autres lois.

Dans ce cadre, le COC procède aux constatations et peut formuler des questions, des recommandations, des avertissements et/ou des mesures correctrices (au caractère contraignant) en tant que *« ultimum remedium »* si le COC constate des infractions aux lois et règlements.

L'Organe de contrôle est en particulier chargé du contrôle du respect des règles relatives à l'accès direct à la Banque de données nationale générale (BNG) et à son interrogation directe, ainsi que du respect de l'obligation visée à l'article 44/7, 3e alinéa de la LFP, qui oblige tous les membres des services de police à alimenter cette banque de données.

À travers une inspection du fonctionnement, l'Organe de contrôle vérifie si le contenu de la BNG et la procédure de traitement des données et informations qui y sont conservées sont conformes aux dispositions des articles 44/1 à 44/11/14 de la LFP et à leurs mesures d'exécution.

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MPR »[7]. Conformément à l'article 46/6 de la LFP, toute autorisation et prolongation d'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée à l'Organe de contrôle sauf lorsque l'utilisation des caméras est réalisée sous le contrôle d'un magistrat. L'Organe de contrôle doit alors examiner si les conditions pour la

---

[1] M.B. 5 septembre 2018. Cette loi contient des dispositions qui donnent exécution au Règlement (UE) 2016/679 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), ci-après dénommée « RGPD » et la 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 (ci-après dénommée « directive Police-Justice » ou LED (**L**aw **E**nforcement **D**irective)).

[2] Le COC établit une distinction entre différentes formes de contrôles ou de surveillance. Le COC procède soit à :

- **un contrôle global :** il s'agit d'un contrôle qui s'assortit d'une ou plusieurs visites approfondies sur place et d'une portée très large ;
- **un contrôle thématique :** comme le nom l'indique, il s'agit d'une enquête menée sur un thème déterminé et qui peut inclure à la fois de la *desk research* et des visites sur place ;
- **un contrôle technique :** il s'agit d'un contrôle qui se concentre sur la licéité, l'exhaustivité et l'exactitude des enregistrements/traitements effectués dans les banques de données policières ;
- **un contrôle restreint :** ce contrôle porte sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier ;
- **un contrôle international :** il s'agit des éventuelles enquêtes internationales auxquelles le COC apporte son concours ;
- **un contrôle spécial :** il s'agit d'un contrôle portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme.

[3] Tels que définis à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (loi sur la police intégrée) et à l'article 26, 7°, a de la LPD.

[4] Telle que définie à l'article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police et à l'article 27, 7°, d de la LPD.

[5] Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers (art. 26, 7°, f de la LPD). BEL-PIU est l'acronyme de la dénomination anglaise '*Belgian Passenger Information Unit*'.

[6] Article 4 §2, troisième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (LAPD).

[7] MPR signifie « méthodes particulières de recherche ».

décision, la prolongation ou l'exécution de cette mesure sont remplies. L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé[8].

Les membres et les membres du personnel de l'Organe de contrôle, dont notamment son 'Service d'Enquête (DOSE)'[9], disposent à cet égard de compétences d'investigation, après quoi l'Organe de contrôle – et plus spécifiquement son comité de direction (DIRCOM) – peut au besoin prendre des mesures correctrices[10].

Un recours juridictionnel peut être introduit dans les trente jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire[11].

1. OBJET DU CONTRÔLE

1. En 2019, l'Organe de contrôle de l'information policière ('l'Organe de contrôle' ou 'le COC') a effectué de sa propre initiative, en collaboration avec le Comité permanent de Contrôle des services de renseignement et de sécurité (Comité R), un contrôle restreint auprès de l'Unité d'Information des Passagers (UIP). Vu ses compétences autonomes en sa qualité d'autorité de contrôle compétente à l'égard des traitements de données effectués par l'UIP, l'Organe de contrôle a de sa propre initiative décidé le 14 octobre 2021 d'effectuer un contrôle spécial auprès de l'UIP.

2. ORGANISATION ET MÉTHODOLOGIE DU CONTRÔLE

2. Le contrôle ne faisait pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) d'un non-respect, par l'UIP visitée, de la législation et de la réglementation.

Le contrôle effectué en 2019 avec le Comité permanent R était un contrôle restreint étant donné que l'UIP n'était opérationnelle que depuis 2018 et que les transporteurs et opérateurs de voyage n'étaient pas encore tous techniquement connectés à l'UIP.

La banque de données des passagers et l'UIP sont cette année (2022) opérationnelles depuis près de quatre ans. De plus, il ressort du rapport annuel 2020 de l'UIP que davantage de compagnies aériennes sont désormais connectées, de sorte que le screening porte sur un plus grand nombre de passagers aériens qu'en 2019[12]. Bien que cela permette un contrôle plus étendu (global), l'Organe de contrôle a choisi d'axer le contrôle sur l'efficacité du traitement des données des passagers.

La Commission européenne s'est déjà livrée à un exercice de révision de la directive PNR[13]. Un exercice similaire sera réalisé à l'échelle de la Belgique pour la loi PNR. Pour cette raison, le contrôle s'est concentré sur la question de la plus-value de la banque de données des passagers en comparaison d'autres méthodes d'enquête, et de la proportionnalité du traitement de données à grande échelle compte tenu de l'ingérence profonde qu'il implique dans la vie privée.

3. Le contrôle et l'enquête ont en l'occurrence été limités à trois domaines :
1. point de la situation et suivi d'une partie du rapport de contrôle de 2020, dont l'établissement des profils ;
2. l'efficacité et la proportionnalité de la banque de données des passagers (la question centrale de l'enquête) ;
3. les requêtes ciblées et les demandes de recherche ciblée.

Le COC s'est pour ce faire limité à la police intégrée (GPI) étant donné qu'il est compétent uniquement pour les traitements policiers effectués par l'UIP. En ce qui concerne les demandes de recherche ciblée, l'enquête a également été limitée aux réquisitions de l'Administration générale des Douanes & Accises.

4. Le contrôle spécial s'est déroulé en trois phases, à commencer par le point de la situation et le suivi du rapport de contrôle de 2020.

---

[8] Art. 240, 4° de la LPD.
[9] **D**ienst **O**nderzoeken / **S**ervice d'**E**nquête.
[10] Art. 244 et 247 de la LPD.
[11] Art. 248 de la LPD.
[12] Voir plus loin, 3.1 La banque de données des passagers.
[13] Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive (UE) 2016/681, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0305:FIN:FR:PDF.

L'Organe de contrôle a par ailleurs interrogé la police fédérale sur ses expériences avec l'UIP et l'utilisation des données des passagers aériens. Un questionnaire a ainsi été transmis à la Police Aéronautique (LPA), qui assure les contrôles aux frontières et la surveillance dans les aéroports belges. Une Police Judiciaire Fédérale (PJF) a en outre été interrogée sur la plus-value de l'utilisation des données des passagers et sur la suite qui est réservée aux *hits* validés qui sont transmis (*matches*).

Lors de l'annonce du contrôle, il a été demandé de fournir au COC quelques profils actifs[14] de 2020 ainsi que leurs résultats. Dans une troisième phase, une visite a été organisée auprès de l'UIP le jeudi 14 octobre 2021. Sur la base des réponses fournies par la police fédérale dans le cadre de la deuxième phase, l'UIP a été interrogée sur l'efficacité et la proportionnalité de la banque de données des passagers. Le COC a eu à ce sujet une réunion avec le fonctionnaire dirigeant, le délégué à la protection des données et les gestionnaires de dossiers de la GPI.

Il convient d'attirer l'attention sur le récent arrêt[15] rendu le 21 juin 2022 par la Cour de Justice de l'Union européenne (arrêt de la Cour dans l'affaire C-817/19, *Ligue des droits humains*), dans lequel la Cour, en réponse à une série de questions préjudicielles de la Cour constitutionnelle belge, indique notamment que les droits fondamentaux exigent que les compétences de traitement prévues par la directive PNR ne peuvent être exercées que dans la mesure où c'est strictement nécessaire. Certaines remarques formulées par la Cour ont également été identifiées par le COC lors de sa visite et sont abordées dans le rapport.
La plupart des remarques de la Cour ont toutefois un impact sur le cadre légal national, notamment en ce qui concerne le champ d'application restreint de la directive PNR, et ne sont donc pas prises en compte dans le présent rapport. Le verdict de la Cour de Justice porte en effet sur un certain nombre de questions préjudicielles posées par la Cour constitutionnelle, et le COC ne peut et ne souhaite pas préjuger dans le rapport du verdict que rendra la Cour constitutionnelle à la lumière de l'arrêt du 21 juin 2022 de la Cour de Justice.

L'UIP a ensuite eu l'occasion de formuler des remarques concernant le rapport et/ou d'indiquer sur quels points les mesures correctrices nécessaires ont dans l'intervalle déjà été prises et ont donc un impact sur les recommandations et/ou mesures correctrices que l'Organe de contrôle a l'intention de formuler. L'UIP a fait usage de cette possibilité dans le délai imparti, et il a été tenu compte de ces remarques lorsqu'elles étaient pertinentes.

3. LE TRAITEMENT DES DONNÉES DES PASSAGERS

5. La Loi du 25 décembre 2016 *relative au traitement des données des passagers* ('la loi PNR') met en œuvre les objectifs européens qui sont à la fois de prévenir et de combattre le terrorisme et les infractions graves et la criminalité transnationale qui y sont liées[16]. À cet effet, une Unité d'Information des Passagers (UIP) a été mise en place au sein du SPF Intérieur. Cette unité conserve les données des passagers dans une banque de données en vue de prévenir et combattre les délits ou menaces prévus par la loi PNR.

3.1. La banque de données des passagers

6. Pour tous les passagers voyageant en Belgique ou partant d'un aéroport belge ou encore voyageant à travers la Belgique en empruntant des trains et bus internationaux, un large éventail de données à caractère personnel est stocké et analysé dans la banque de données des passagers par rapport à un nombre limité de délits ou de menaces. La banque de données des passagers est une banque de données centralisée qui est gérée par le SPF Intérieur, le fonctionnaire dirigeant de l'UIP étant désigné au titre de responsable du traitement.

Les données des passagers doivent être transmises à l'UIP par les compagnies aériennes, les transporteurs de passagers et les opérateurs de voyage 48 heures avant le départ ou l'arrivée en Belgique[17]. De manière générale, il s'agit de deux

[14] Voir plus loin au point 10.
[15] https://curia.europa.eu/juris/document/document.jsf;jsessionid=650151DB421A7F88628FE6238F6052F7?text=&docid=261282&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=5680444.
[16] La loi PNR transpose la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière ('la directive PNR') et la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers ('la directive API').
[17] Trois arrêtés d'exécution régissent les obligations des compagnies aériennes, des transporteurs HST et des distributeurs de tickets HST et des transporteurs par bus internationaux (l'arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les transporteurs par bus, *M.B.* 12 février 2019 ; l'arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les transporteurs HST et les distributeurs de tickets HST, *M.B.* 12 février 2019). Le transport maritime international sera encore ajouté à un stade ultérieur (voir l'arrêté royal du 18 juillet 2017 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les compagnies aériennes, *M.B.* 28 juillet 2017, et l'arrêté royal du 21 décembre 2017 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données, *M.B.* 29 décembre 2017).

catégories de données, à savoir les données API (*Advanced Passenger Information*) ou les données d'enregistrement et d'embarquement (numéro de la carte d'identité ou du passeport, nom, prénom et date de naissance, etc.) et les données PNR (*Passenger Name Records*) ou les données de voyage des passagers (nom et adresse, numéro de vol, destination, modalités de paiement, numéro de siège dans l'avion, heure de départ et d'arrivée, etc.).

7. Depuis la création de l'Unité d'Information des Passagers (UIP) en 2018, plus de 50 millions de 'données passagers' ont ainsi été traitées dans la banque de données des passagers. Le terme 'données passagers' doit, tout comme dans notre rapport précédent, être nuancé. On entend en effet par là le nombre de déplacements enregistrés. Un passager est enregistré dans la banque de données des passagers à chaque déplacement qu'il effectue. Un passager qui effectue par exemple un déplacement aller-retour sur une certaine destination sera par conséquent enregistré deux fois dans la banque de données des passagers, ce qui signifie qu'une même personne peut figurer plusieurs fois dans cette banque de données.

Depuis 2020, les cinq principaux aéroports de Belgique et environ 70 % des compagnies aériennes opérant en Belgique sont techniquement connectés à l'UIP pour la fourniture de données PNR et API. Il en découle que depuis la fin 2020, 98 %[18] des passagers qui prennent l'avion au départ ou à destination de la Belgique sont enregistrés dans la banque de données des passagers[19]. Vu l'énorme banque de données dont dispose l'UIP, il va donc de soi que le traitement des données doit faire l'objet d'un contrôle interne et externe effectif et adéquat. Vu l'envergure de la banque de données, la nature des données et la forme des traitements effectués par l'UIP, il s'agit en effet d'une ingérence profonde dans la vie privée.[20]

3.2. L'Unité d'Information des Passagers (UIP)

8. L'UIP est placée sous le contrôle fonctionnel d'un fonctionnaire dirigeant du SPF Intérieur. Elle est composée d'un service d'appui et de membres détachés de la Police intégrée (GPI), de la Sûreté de l'État (VSSE), du Service Général du Renseignement et de la Sécurité (SGRS) et de l'Administration générale des Douanes et Accises (AGDA). Le centre névralgique est l'*Operational Travel Intelligence Room* (*OTIR*), un espace où les membres détachés ont accès à la banque de données des passagers, également appelée métaphoriquement *closed box*. Dans l'optique du législateur, il s'agit d'un espace hermétiquement fermé aux tiers et aux personnes non autorisées qui n'est accessible qu'à un nombre limité de personnes spécifiquement désignées ; l'accès à la banque de données des passagers est lié à l'exécution d'une mission spécifique par le membre détaché de l'UIP. Par conséquent, le membre détaché n'a accès qu'aux données des passagers relatives à la ou aux affectations de son service, et ce sur la base de profils d'accès individuels.

3.3. Le processus de traitement des données

9. Le traitement des données des passagers par l'UIP peut être divisé en trois composantes : (1) le contrôle des personnes ou des objets connus, pour lesquelles ou auxquels une mesure policière ou judiciaire est associée ou qui sont suivis par les services de renseignement ou les douanes, (2) l'identification de passagers liés sur la base de critères de déplacements suspects en rapport avec un crime ou une menace et (3) la disponibilité des données pour les enquêtes ciblées, les enquêtes de renseignement et la coopération internationale.

Après réception des données des passagers par l'UIP, les données sont automatiquement comparées à la *watchlist* ou aux listes de noms établies par la GPI, la VSSE, le SGRS ou l'AGDA (seul ou conjointement).

10. En outre, les données des passagers, sous réserve de l'autorisation du fonctionnaire dirigeant de l'UIP, peuvent également être liées à des critères d'évaluation objectifs (profils) préalablement établis par un service de police ou par les membres détachés, conjointement ou non. Les données des passagers peuvent également être utilisées à cette fin. Ces critères doivent être ciblés, c'est-à-dire avoir pour but d'identifier un (des) suspect(s) potentiel(s) dans le cadre d'une enquête. Ils doivent également être proportionnés en fonction du crime ou de la menace ciblé(e) par le profil. Les critères doivent être suffisamment spécifiques pour exclure au maximum le risque de *hit* erroné. Il s'agit d'un ou de plusieurs indicateurs objectifs dont on peut déduire que les personnes répondant à ce profil présentent un risque (spécifique) pouvant être associé à un ou plusieurs délits ou menaces énuméré(e)s dans la loi PNR. L'évaluation préliminaire peut également se fonder sur une analyse d'autres données relatives à des passagers en lien avec une correspondance positive. Il est ainsi possible de découvrir d'éventuels passagers liés suspects.

---

[18] Chiffre communiqué par l'UIP le 8 septembre 2022.

[19] Rapport annuel 2021 de l'UIP.

[20] À savoir les articles 7 (protection de la vie privée) et 8 (protection des données à caractère personnel) de la Charte des droits fondamentaux de l'Union européenne et l'article 22 de la Constitution. Outre les données d'identification, l'UIP traite ainsi également les données de paiement et le comportement de voyage des passagers.

Cependant, le profil ne doit pas viser à identifier un passager spécifique ou être basé sur l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, les opinions politiques, l'affiliation à un syndicat, l'état de santé, la vie sexuelle ou l'orientation sexuelle de la personne.[21]

11. En cas de résultat positif (*hit*) basé sur une correspondance avec la *watchlist* du service compétent ou le profil (critères d'évaluation), il doit être validé par le fonctionnaire détaché auprès de l'IUP dans les 24 heures (*match*). Les *hits* ne sont accessibles (visibles) qu'aux membres détachés du service compétent, ce qui n'exclut pas que le *hit* puisse concerner différents services (*hit* commun). Le *hit* validé est enrichi avec des données PNR pertinentes avant d'être transmis aux services compétents respectifs pour suite utile. Dans ce contexte, l'UIP ne transmet pas encore de données de passagers[22] à la Police des frontières et à l'Office des étrangers dans l'exercice de leurs fonctions dans le cadre des contrôles aux frontières extérieures et de l'application de la réglementation sur le séjour et l'asile parce qu'aucun arrêté d'exécution n'a encore été promulgué. Dans le cas d'un *hit* multiple (*hit* provenant de plusieurs profils établis par des services différents), l'UIP organise sur une base volontaire une concertation interne entre les différents services qui ont établi le profil[23].

Le résultat *négatif* (donc l'absence de *match*) est conservé pour la période qui s'applique à toutes les données des passagers, à savoir 5 ans. Le législateur veut ainsi pouvoir éviter les fausses correspondances positives.[24]

12. Comme indiqué ci-dessus, les données PNR peuvent être obtenues sur la base d'une requête motivée du Ministère public, sur la base d'une décision motivée du dirigeant du service de renseignement et de sécurité[25], ou sur la demande motivée du conseiller général de l'AGDA, dans le cadre de recherches ciblées liées à une infraction ou à une menace au sens de la loi PNR et en vue d'un échange de données à l'étranger dans le cadre d'une demande d'entraide internationale.[26] Il s'agit de dossiers concrets, dans lesquels la connaissance des données des passagers (mode de réservation, modes de déplacement et destination) d'une personne ou d'un groupe spécifique est pertinente pour l'instruction pénale ou l'enquête de renseignement.

13. Les données passagers sont dépersonnalisées par l'UIP six mois après leur enregistrement (même si elles peuvent être conservées pendant 5 ans). Cela signifie que les données sont protégées de manière à ce que le passager ne soit plus directement individualisable. Les données ne peuvent être repersonnalisées que dans le cadre d'une recherche ciblée. Les données passagers doivent être détruites[27] après la période de conservation de 5 ans. L'UIP n'étant opérationnelle que depuis début 2018, les premières données de passagers devraient être supprimées de la banque de données des passagers d'ici début 2023.[28]

14. Compte tenu du caractère sensible des données traitées en termes de confidentialité, des exigences élevées sont fixées en matière de sécurité de l'information. En plus de l'attention accordée à l'intégrité, la fiabilité, la confidentialité et la disponibilité des données, cela concerne également la sécurité physique et organisationnelle. Dans ce contexte, un rôle important a été attribué au délégué à la protection des données (DPO, *Data Protection Officer*)[29], qui doit effectuer les contrôles (proactifs) requis. Le DPO a également un rôle de conseil vis-à-vis du responsable du traitement. Il a en outre accès à toutes les informations pour pouvoir mener à bien ses missions et en rendre compte au fonctionnaire dirigeant et au ministre de l'Intérieur. À cet égard, il sert de point de contact pour l'Organe de contrôle.

Le respect des obligations énoncées dans la loi PNR et les arrêtés d'exécution incombe au responsable du traitement, en particulier au fonctionnaire dirigeant de l'UIP.[30]

4. CONCLUSIONS DE L'ENQUÊTE

[21] Articles 24 §2 et 25 de la loi PNR.
[22] Il s'agit concrètement des données API (*Advance Passenger Information*) qui font partie de la liste globale des données PNR telle que visée à l'article 9 de la loi PNR.
[23] Article 8 §1er de l'arrêté royal du 21 décembre 2017 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données.
[24] Article 21 §3, deuxième alinéa de la loi PNR.
[25] Voir également à cet égard l'article 16/3 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Toute recherche ciblée doit être motivée et le Comité permanent R peut interdire l'utilisation de données collectées illégalement.
[26] Article 27, article 51 et Chapitre 12 de la loi PNR.
[27] Article 18 de la loi PNR.
[28] Article 30, alinéa 2 de la LPD *juncto* article 5 de la Directive Police et Justice.
[29] Arrêté royal du 21 décembre 2017 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données, *M.B.* 29 décembre 2017.
[30] Article 15 §2 de la loi PNR.

4.1. Suivi du rapport de contrôle de 2020

15. Dans le rapport de contrôle de 2020, le Comité R et l'Organe de contrôle formulaient à l'adresse de l'UIP un certain nombre de recommandations, qui ont été passées en revue et abordées lors de la visite rendue à l'UIP.

4.1.1. Sécurisation de l'infrastructure ICT

16. Le COC constate lors de la visite sur place que l'infrastructure ICT n'a toujours pas été soumise à un audit (recommandation n° 3 du rapport de contrôle de 2020). L'UIP garantit au COC qu'il y sera procédé dans les meilleurs délais. Dans sa réponse au projet de rapport, l'UIP indique faire dans l'intervalle l'objet d'un audit approfondi de son infrastructure ICT et de sa politique de sécurité de l'information. Le COC en prend acte, ainsi que de l'intention de l'UIP de tenir le COC informé.

4.1.2. Définition des critères d'évaluation (profils)

17. Le COC constate que l'UIP applique pour les profils un certain nombre de garanties additionnelles en plus de celles prévues dans la loi PNR.

Pour commencer, l'UIP vérifie pour chaque profil si le service compétent a besoin d'informations concernant ce profil. Si ce n'est pas ou plus le cas, le profil est supprimé. L'UIP demande aussi du feed-back aux 'destinataires' afin d'évaluer si les critères d'un profil existant doivent éventuellement être adaptés. Pour chaque *match* transmise à la LPA ou à la PJF, un feed-back est formulé.

Par ailleurs, l'UIP veille à ce que les personnes qui génèrent erronément un *hit* (faux positifs) ne fassent pas à chaque fois à nouveau l'objet d'une intervention à l'aéroport sur la base du profil. Les faux positifs sont en effet, tout comme les autres données de passagers, conservés pendant cinq ans.

De plus, les résultats des profils qui ont été établis par la PJF sont uniquement envoyés à la PJF concernée et ne sont pas transmis également à la LPA Contrôle, en dépit du fait que ce résultat pourrait aussi être utile à la Police Aéronautique (LPA). Il en va de même si le profil a uniquement été établi par la LPA Contrôle. L'UIP souhaite ainsi se conformer au principe de la minimalisation des données (qui n'est d'ailleurs pas normalisé au Titre 2 de la LPD[31]).

18. Ces garanties additionnelles doivent permettre d'éviter que le passager ne subisse un préjudice disproportionné du fait du traitement de ses données de passagers. Le COC ne peut qu'approuver cette prise de conscience et cette volonté d'optimaliser les processus de travail en vue de créer un équilibre acceptable entre les intérêts en présence et les droits et libertés fondamentaux. Pour la transparence et la prévisibilité, il est indiqué d'inscrire dans la loi PNR ces garanties additionnelles et ces critères potentiels (qui sont dans la pratique déjà appliqués). Le citoyen pourra en effet ainsi raisonnablement mieux évaluer dans quelles circonstances et dans quelles conditions il pourrait (ou non) relever d'un profil donné (prévisibilité). Cela rejoint en outre la jurisprudence (européenne) qui dispose que la base légale doit satisfaire à certaines exigences de qualité. Il s'agit d'un exercice dynamique qui revient au législateur, en fonction de la mesure (croissante) de l'atteinte aux droits et libertés fondamentaux du citoyen dans le contexte de la lutte contre les formes graves de criminalité et le terrorisme, et qui rejoint également le considérant 210 de l'arrêt du 21 juin 2022 de la Cour de Justice de l'Union européenne.

4.2. Proportionnalité et efficacité de la banque de données des passagers

19. Selon le rapport annuel 2020 de l'UIP, il existe d'une part un écart significatif entre le nombre de correspondances positives (*hits*) et la validation (*matches*) au niveau de l'UIP, et d'autre part un écart substantiel entre le nombre de *matches* transmises à la police et le nombre de *matches* conduisant effectivement à un 'contrôle'[32]. Il est donc important que les responsables du traitement respectifs examinent à quoi sont dus ces écarts afin de pouvoir vérifier l'efficacité de la banque de données des passagers.

Le considérant 106 de l'arrêt du 21 juin 2022 de la Cour de Justice de l'Union européenne fait référence au document de travail de la Commission européenne (SWD(2020) 128 final) portant réexamen de la directive PNR de 2016, selon lequel *« le nombre de cas de concordances positives résultant des traitements automatisés prévus à l'article 6, paragraphe 3, sous a) et b), de cette directive qui se sont révélées erronées après réexamen individuel par des moyens non automatisés est assez conséquent et s'élevait, au cours des années 2018 et 2019, à au moins cinq personnes sur*

[31] Contrairement au RGPD (article 5.1. c) du RGPD).
[32] Selon l'article 24 §5 de la loi PNR, une suite utile doit toujours être donnée à un *hit* validé. Une suite utile ne doit pas nécessairement être un contrôle, mais peut aussi consister en la mise en œuvre d'une mesure à prendre, un refus de l'accès à un territoire, un contrôle ciblé/discret, une arrestation, la collecte d'informations, l'établissement d'un RIR/PV/BR, etc.

six identifiées ». Le COC tient toutefois à souligner que cet écart substantiel n'a pas été constaté dans la même mesure auprès de l'UIP dans le cadre des visites effectuées en 2020 et 2021 (voir plus loin).

4.2.1. Vols au sein de l'espace Schengen et en dehors de l'espace Schengen

20. En marge du système PNR, la Belgique dispose de tout un arsenal de méthodes d'enquête ou de recherche permettant d'identifier certaines formes de criminalité (aux frontières). Il peut s'agir des 'Mesures à Prendre' (MAP) ou signalements dans la BNG ou les banques de données particulières, de *watchlists* des entités de la GPI, des signalements dans le système SIS, des signalements Interpol, etc.

21. Dans l'optique des finalités pour lesquelles la banque de données des passagers a été créée, elle présente l'avantage (dans le cas de vols en dehors de l'espace Schengen) que le système PNR, en comparaison des autres banques de données policières, permet à la police d'intervenir plus rapidement lorsqu'un criminel (potentiel) entre dans le pays ou en sort. Pour les vols en dehors de l'espace Schengen, les services de police seraient, sans le système PNR, informés du déplacement de cette personne seulement lors de l'atterrissage de son avion en Belgique et ne seraient donc pas en mesure de préparer l'intervention, à moins d'une coopération policière transfrontalière concrète. On peut toutefois se demander si sa plus-value est objectivement mesurable – et, dans l'affirmative, dans quelle mesure – afin de justifier l'ingérence profonde de la banque de données des passagers dans la vie privée.

22. Pour les vols au sein de l'espace Schengen, par contre, le système PNR est presque la seule forme de contrôle des frontières intérieures de l'UE, à moins d'une coopération policière transfrontalière concrète. Voyager entre les pays de l'espace Schengen peut en effet en principe se faire librement, et donc sans que les données à caractère personnel ne soient enregistrées dans la banque de données des passagers et utilisées. En principe, il n'y a pas non plus de contrôle de police dans ce cas de figure. La Belgique a par conséquent introduit cette obligation PNR également pour les vols au sein de l'UE, qui représentent trois quarts (75 %) du nombre total de déplacements[33]. La directive PNR laisse en effet aux États membres la liberté d'étendre ou non cette obligation aux vols au sein de l'UE[34]. De l'avis des décideurs politiques européens, cette extension permet en outre d'éviter que le risque de menace terroriste se déplace au lieu d'être éliminé, dès lors que les terroristes rejoignent de plus en plus souvent leur destination par des voies détournées[35].

4.2.2. Transmission à la police fédérale

23. Les données PNR sont automatiquement liées à la BNG et aux banques de données communes (BDC)[36]. Les données PNR reçues sont liées à des personnes qui ont été enregistrées pour un ou plusieurs faits relevant des délits visés par la loi PNR, pour autant que ces personnes fassent l'objet d'une mesure à prendre (arrestation, contrôle, …). Pour expliquer le système simplement, il est recouru à des filtres qui répondent aux finalités de la loi PNR et la corrélation génère des *hits* et des *no hits*. Le résultat n'est accessible (visible) qu'aux membres détachés de la police intégrée.

Une fois qu'un *hit* a été validé par le membre détaché de la police intégrée au niveau de l'UIP, la *match* est transmise à la police fédérale. En règle générale, tous les *hits* validés sont transmis à la Police Aéronautique (LPA), c'est-à-dire à l'entité de la LPA de l'aéroport belge concerné. Si toutefois le *hit* découle d'une *watchlist* ou d'un profil établi dans le cadre d'un dossier judiciaire par la Police Judiciaire Fédérale (PJF), le *hit* validé est transmis à la PJF concernée. Le résultat de l'intervention est ensuite communiqué à l'UIP.

4.2.3. Dans le cadre des contrôles aux frontières

24. Au sein de la Police Aéronautique, les *matches* (*hits* validés) sont ensuite transmises aux unités sur le terrain – en l'occurrence à l'aéroport – en vue d'une action policière. Dans le cadre de son enquête par échantillonnage, le COC a interrogé uniquement la Police Aéronautique de l'aéroport de Zaventem. Dans près de la moitié des cas, les *matches*

[33] Rapport annuel 2021 de l'UIP.
[34] Considérant 10 de la directive PNR.
[35] CONSEIL DE L'UE, Note du 4 avril 2011 concernant la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière – L'inclusion éventuelle des vols au sein de l'UE, p. 3. Selon la Commission européenne, tous les États membres, à une exception près, ont eu recours à cette extension facultative aux vols intra-Schengen (COMMISSION EUROPÉENNE, Rapport sur le réexamen de la directive PNR, 2020, 20200724_com-2020-305-review_fr.pdf (europa.eu), p. 11). Voir toutefois les conditions imposées entretemps par la Cour de Justice dans son arrêt du 21 juin 2022.
[36] Les banques de données communes contiennent actuellement les noms de tous les combattants terroristes et propagandistes de haine connus de notre pays.

ont donné lieu à des interventions policières et il a été ordonné de procéder à une intervention ou à une observation (46 % du nombre total de *matches* transmises[37]). Dans les autres cas, il ressort des informations fournies au COC par la police de l'aéroport de Zaventem qu'aucune action n'a été entreprise parce que :

1. le *hit* est arrivé trop tard ;

   les compagnies aériennes doivent transmettre les données API et les données PNR à l'UIP 48 heures avant le départ ou l'arrivée en Belgique.

2. le *hit* ne concernait pas la bonne personne ;

   c'est par exemple le cas lorsque l'équipe se retrouve face à un vieil homme alors que la personne recherchée est censée être un jeune homme.

   Dans sa réponse au projet de rapport, l'UIP fait remarquer que cela ne peut arriver que lorsque le *hit* est lié à l'enregistrement de la personne dans la banque de données commune[38], mais pas pour un *hit* dans la BNG étant donné qu'une date de naissance est toujours demandée dans ce dernier cas. Par ailleurs, l'UIP souligne dans cette même réponse qu'elle transmet évidemment uniquement les *hits* ayant trait aux délits prévus par la loi PNR.

   Un deuxième problème qui se pose est que les compagnies aériennes ne contrôlent pas suffisamment soigneusement les cartes d'identité lors de l'enregistrement ou de l'embarquement. La loi oblige les transporteurs et les opérateurs de voyage à garantir que les données de passagers transmises sont complètes, correctes et actuelles, et à contrôler la correspondance entre les documents de voyage et l'identité des passagers concernés[39], mais cette obligation n'est pas respectée dans tous les pays.

3. à l'arrivée de l'avion en Belgique, on a constaté que le passager n'était pas à bord de l'avion ou n'avait pas été enregistré ;

   cette situation se présente pour un quart (27 %)[40] du nombre total de *matches.* Cette donnée (le fait que le passager n'est pas présent) n'est actuellement pas encore transmise par les compagnies aériennes à l'UIP. La Direction de l'information policière et des moyens ICT (DRI) de la police fédérale développe en ce moment des outils qui indiqueront en temps utile aux entités compétentes si le passager a embarqué à bord de l'avion[41].

4. la 'Mesure à Prendre' (MAP) n'est plus *up-to-date* ou le *hit* n'est pas (ou plus) pertinent lors du franchissement de la frontière ;

   il s'agit de mesures qui pour diverses raisons auraient dû être archivées ou effacées, par exemple parce que la mesure n'est plus pertinente ou parce que le délai de conservation est dépassé. La raison en est que la BNG ou la BDC n'a pas été corrigée ou n'a pas été correctement tenue à jour, ce qui génère un faux positif lors de l'interconnexion avec la banque de données des passagers. Selon la LPA, une MAP ayant trait à une interdiction professionnelle ou à une interdiction de conduire pourrait également relever de cette catégorie[42]. Cela signifie que des mesures qui ne sont pas visées par la loi PNR généreraient également un *hit* dans la banque de données PNR, qui serait ensuite validé et transmis. Le COC n'a toutefois pas pu constater un tel cas.

---

[37] Personne interceptée (35 %), traitement de la *match* (6 %), contrôle effectué (4 %).

[38] Telle que visée à l'article 44/11/3*bis* de la LFP, concrètement les banques de données communes '*Terrorist Fighters'* et 'Propagandistes de haine' (arrêté royal du 23 avril 2018 *« modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1re bis « De la gestion des informations » du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters »* ; arrêté royal du 23 avril 2018 *« relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1re bis « De la gestion des informations » du chapitre IV de la loi sur la fonction de police »*. 'Extrémistes Potentiellement Violents' et 'Personnes condamnées pour terrorisme' (arrêté royal du 20 décembre 2019 *« modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1re bis « De la gestion des informations » du chapitre IV de la loi sur la fonction de police »*).

[39] Article 7 §§ 1er et 2 de la loi PNR.

[40] Passager pas à bord (25 %) + Passager pas enregistré (2 %).

[41] Note de la LPA Brunat (Titre 5. Renseignements complémentaires).

[42] Réponse de la LPA Brunat (point 1a).

5. en raison d'un manque de capacité ;

   parce que la priorité est à ce moment accordée à un autre dossier ne présentant aucun lien avec l'UIP. Aucune politique d'action et d'intervention définitive n'a cependant été élaborée à cet effet par la LPA.

4.2.4. Dans le cadre de dossiers judiciaires

25. Pour pouvoir établir la plus-value concrète des données PNR dans une enquête judiciaire, le COC a demandé à l'UIP de lui communiquer un profil concret au titre d'étude de cas. Ce profil a été établi dans le cadre d'une enquête proactive à la demande d'un magistrat conformément à l'article 28*bis* §2 du Code d'instruction criminelle. L'assistance de l'UIP a également été sollicitée.

26. La situation est la suivante: si un *hit* est généré à partir de ce profil établi, le membre détaché validera ce *hit* en sa qualité de membre détaché et établira un rapport confidentiel en sa qualité de fonctionnaire de police de la PJF[43]. Ce rapport confidentiel sera ensuite conservé au niveau de la PJF en charge de l'enquête proactive, après quoi le *hit* sera également consigné dans un procès-verbal[44]. En l'occurrence, les *hits* n'ont donc pas été transmis à la PJF mais ont déjà été analysés au niveau de l'UIP, de sorte que l'UIP prend *de facto* part à l'enquête proactive et accomplit donc bel et bien des devoirs d'enquête[45]. Les deux membres détachés de l'UIP agissent par conséquent d'une part en tant que membres détachés de l'UIP et d'autre part en tant que fonctionnaires de police de la PJF dont ils faisaient initialement partie.

27. Le COC entrevoit ici deux points d'attention : d'une part la question de savoir s'il est opportun, ou si l'intention du législateur est (ou était) de faire porter une double casquette aux membres détachés de la GPI. Une fois détaché, le fonctionnaire de police conserve il est vrai son statut, mais il exerce en principe pendant la durée de son détachement les compétences de police qui lui ont été attribuées dans et par la loi PNR[46]. L'établissement d'un rapport confidentiel ou d'un procès-verbal dans le cadre d'une information en cours ne relève en principe pas des missions du fonctionnaire de police détaché telles que définies dans la loi PNR ; la loi PNR ne le prévoit du moins pas, et l'attention est attirée sur le fait que la finalité de la banque de données des passagers est strictement délimitée.

Dans cette optique, il semble pour le moins frappant, également d'un point de vue juridique, que l'UIP fasse partie des services de police qui mènent cette enquête proactive. Le COC se pose des questions quant à la conformité légale de cette configuration, précisément parce que la loi PNR poursuit des objectifs spécifiques. L'UIP (et donc aussi ses membres) est (sont) en effet uniquement en charge de la collecte et du traitement des données de passagers transmises, de la gestion des banques de données de passagers et de l'échange de données de passagers ainsi que des résultats de ces opérations[47]. Il s'agit d'une compétence liée qui doit en tout état de cause faire l'objet d'une interprétation restrictive. Les services de police saisis se mettent ensuite au travail avec ces données (interventions des services de police et utilisation par la police judiciaire). L'article 28*bis* §2 du Code d'instruction criminelle dispose en outre que l'enquête proactive fait partie de l'information. Strictement parlant, l'article 28*ter* §3 du Code d'instruction criminelle prévoit ensuite que le procureur du Roi a le droit de requérir les **services de police** visés à l'article 2 de la LFP et tous les autres officiers de police judiciaire. L'UIP n'est de toute évidence pas un service de police. La question de savoir si les fonctionnaires de police détachés de l'UIP sont des officiers de police judiciaire doit pour sa part être examinée au cas par cas. Par ailleurs, le procureur peut en vertu de l'article 28*ter* §4 désigner les **services de police** chargés des missions de police judiciaire dans une enquête particulière. Si plusieurs « services de police » sont désignés, le procureur du Roi veille à la coordination de leurs interventions. Ici aussi, nous ne pouvons que constater que l'UIP n'est pas un service de police au sens du paragraphe 4 de l'article 28*ter* du Code d'instruction criminelle. De plus, l'article 46*septies* du Code d'instruction criminelle encadre plus spécifiquement les réquisitions de l'UIP et prévoit que le procureur du Roi peut, en recherchant les crimes et délits visés par la loi PNR, charger l'officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers. Ni plus, ni moins. L'établissement de procès-verbaux et/ou de rapports confidentiels n'est manifestement pas prévu par l'article 46*septies* du Code d'instruction criminelle, qui décrit également une compétence spécifique et liée.

Deuxièmement et à titre subsidiaire, le COC ne voit pas tout à fait, à la lumière de ce qui précède, quel est le fondement juridique de l'établissement d'un rapport confidentiel par l'UIP. La situation dans laquelle un rapport confidentiel peut

[43] Courrier de l'UIP du 15/11/2021 (point 5).
[44] Courrier de l'UIP du 09/12/2021.
[45] Réponse de l'UIP du 15/11/2021.
[46] Article 14 §1er, dernier alinéa de la loi PNR.
[47] Article 13 §1er de la loi PNR.

être établi se situe selon le Code d'instruction criminelle dans le cadre des méthodes particulières de recherche (MPR)[48]. À côté de cela, et donc en dehors de l'application de la loi concernant les MPR, l'établissement d'un 'rapport confidentiel' est également réglementé dans la fiche B51 non publiée – et donc interne – de la directive commune MFO-3 qui s'intitule 'Établissement de rapports confidentiels'[49]. La conservation des *hits* (non pertinents) par la police judiciaire fédérale ne semble cependant pas remplir les conditions imposées par cette fiche B51, qui énonce trois situations dans lesquelles un rapport confidentiel peut être établi par la GPI (en dehors du cas de l'application de la loi concernant les MPR). De plus, les *hits* qui ne présentent aucun lien avec l'information ne sont pas conservés (plus longtemps).

D'un autre côté, le COC comprend que l'UIP, comme il ressort de sa réponse au projet de rapport, perçoit à cet égard sa collaboration consistant en l'établissement de profils purement comme un soutien à l'enquête proactive dans la mesure où le Ministère public l'implique dans l'information. Cependant, il ressort clairement de ce qui précède qu'il est difficile, pour ne pas dire impossible, de délimiter la frontière entre d'une part les compétences générales et particulières de la police et d'autre part les compétences strictement définies de l'UIP (dont font partie les fonctionnaires de police détachés). Vu la délimitation stricte des objectifs de la directive PNR[50] et des compétences liées de l'UIP, on pourrait difficilement admettre que celles-ci puissent dans les faits faire l'objet d'une interprétation extensive. Comme l'affirme la Cour de Justice, l'atteinte à la vie privée et à la protection des données à caractère personnel doit, à la lumière de la gravité de l'atteinte aux droits fondamentaux, être régie par des règles claires et précises quant à leur portée et à leur application.

Le COC est donc d'avis qu'il est primordial pour la sécurité juridique que le législateur, si l'intention est effectivement de faire également relever l'UIP de l'application des §§ 3 et 4 de l'article 28*bis* du Code d'instruction criminelle, prenne l'initiative de réglementer clairement cet aspect dans la loi PNR, en supposant que la délimitation des finalités de la directive PNR soit ainsi respectée.

28. Pour le reste, ce profil a généré 1000 *hits*, dont les plus « intéressants » ont été abordés et partagés avec la GPI. La suite concrète réservée à ces *hits* n'est pas clairement établie, mais ces 1000 *hits* seraient tous, après analyse, consignés dans un procès-verbal et contribueraient à l'enrichissement du dossier proactif.[51] Les *hits* ne restent toutefois « utiles » que lorsqu'ils présentent une complémentarité avec d'autres devoirs d'enquête[52]. Le COC insiste sur le fait que les *hits* doivent être pertinents, et donc pas seulement 'utiles', ce qui signifie que la pertinence de cet enrichissement est véritablement examinée.

Dans sa réponse au projet de rapport, l'UIP maintient que les 1000 *hits* étaient bel et bien utiles et pertinents dans le dossier en question. Le COC ne peut que faire remarquer qu'il ressort justement de ce qui précède que cette affirmation n'a pas pu être établie de manière claire ou objectivable.

29. Partant de la perspective de la police, la nature du dossier judiciaire détermine également quels types de *hits* sont utiles à la PJF[53]. Dans le cadre d'un 'dossier d'imagerie'[54], l'objectif est de se faire une idée d'un phénomène ou d'un groupement donné, et les données de passagers remontant jusqu'à trois ans peuvent revêtir une importance. Dans ce cas, la PJF adressera à l'UIP une demande de recherche ciblée. Dans les 'dossiers tactiques en cours', en revanche, l'accent est plutôt mis sur les déplacements futurs d'un suspect donné dans le dossier, de sorte que ce sont plutôt les données de passagers récentes remontant à maximum un mois qui seront pertinentes.

Avant la création de la banque de données des passagers et de l'UIP, la PJF devait contacter séparément chaque compagnie aérienne au moyen d'une apostille. Le contenu du dossier était ainsi dans une certaine mesure diffusé, ce qui compromettait la confidentialité des données. Ce problème est à présent résolu grâce à l'existence d'une organisation de contact unique, à savoir l'UIP.

De plus, l'importance des contacts avec les UIP des pays voisins a augmenté dans des proportions exponentielles, parallèlement à l'augmentation de la criminalité transfrontalière. Il va de soi qu'un criminel n'utilisera pas à chaque fois

---

[48] Article 47*septies* §1er du Code d'instruction criminelle.

[49] Directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur *« relative à la gestion de l'information de police judiciaire et de police administrative »* (*M.B.* 18 juin 2002).

[50] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

[51] Réponse de l'UIP du 09/12/2021.

[52] Réponse de la LPA Bruxelles-National du 06/12/2021.

[53] Au surplus, « utile » n'a pas la même signification que « pertinent » au sens des articles 28 de la LPD et 44/1 §1er de la LFP.

[54] Il peut ici uniquement s'agir :

- soit d'un dossier purement policier (avant qu'une information ne soit ouverte) = limité dans le temps ;
- soit d'une information (enquête proactive ou non).

Un « dossier d'imagerie » peut être aussi bien l'un que l'autre. Un dossier tactique en cours sera plutôt une information.

le même aéroport, mais préférera alterner avec les aéroports de pays voisins comme Schiphol aux Pays-Bas, Charles-de-Gaulle en France, etc.

4.2.5. Données à caractère personnel de personnes non suspectes

30. Jusqu'ici, nous avons parlé de ce qu'il advient des *hits* validés (*matches*) qui conduisent à l'enrichissement d'une information, mais l'on peut aussi se demander ce qu'il advient des données à caractère personnel de suspects potentiels qui ne peuvent pas être mis en relation avec l'infraction ou le délit. Cette situation peut se produire dans deux cas :

- Le premier cas est la situation où la personne génère un *hit* sur la base de profils en raison de ses déplacements, mais où il s'avère par la suite que cette personne ne présente aucun lien avec une enquête pénale. La GPI n'a pas été en mesure de dire au COC ce qu'il advient des données de cette personne dans une telle situation.
- Dans la deuxième situation, la personne est déjà un suspect dans une information ou dans une instruction judiciaire. La GPI adresse alors une demande de recherche ciblée ou place la personne sur une *watchlist*. L'observation des déplacements permet d'établir que ce suspect ne peut pas être mis en relation avec un délit visé par la loi PNR. Le service de police y voit l'avantage que grâce aux données PNR, cette personne fait moins longtemps l'objet d'une enquête et peut par conséquent être exclue en tant que suspect.

À cet égard, il convient de faire remarquer que le COC, dans le cadre de sa compétence de décision en ce qui concerne les réquisitions de recherches ciblées adressées par le conseiller général désigné du Service Contentieux de l'Administration générale des Douanes et Accises (ci-après 'le conseiller général')[55], examine pour chaque réquisition – ne serait-ce que marginalement – s'il existe un lien entre l'intéressé, le délit et les déplacements en avion. L'objectif du mécanisme du traitement des données de passagers n'est en effet pas de vérifier si la personne n'a pas effectué de déplacements en avion, une conclusion que l'on peut également tirer de l'arrêt du 21 juin 2022 de la Cour de Justice de l'Union européenne.

4.3. Requêtes ciblées

4.3.1. Demandes en provenance de l'étranger

31. L'UIP peut également recevoir des demandes en provenance de l'étranger en vue de transmettre certaines données de passagers ou *hits*[56]. L'UIP contrôle alors la motivation des requêtes et le lien qu'elles présentent avec la Belgique. S'il n'existe aucun lien avec la Belgique ou si la motivation est insuffisante, elle refusera d'accéder à la demande. L'UIP a par ailleurs une règle interne qui stipule que seules des données remontant à maximum six mois peuvent être échangées avec des états membres de l'UE. Cette limitation à six mois est un régime plus strict que celui prévu dans la loi PNR, qui autorise aussi la transmission de données de passagers remontant à plus de six mois[57].

4.3.2. Réquisitions de l'Administration générale des Douanes & Accises

32. Le représentant des douanes au sein de l'UIP reçoit parfois aussi, en même temps que les autres données des passagers, l'« adresse IP » du système informatique ayant servi à la réservation du vol. Selon l'UIP, cette information peut être classée dans la catégorie des 'Remarques générales' telle que définie à l'article 9 §1er, 12° de la loi PNR[58]. L'UIP semble ici faire usage de la formulation très large de cette catégorie. L'Organe de contrôle est pour sa part d'avis que cette catégorie ne saurait être considérée comme une forme de 'catégorie résiduelle' qui autoriserait le traitement d'autres données n'étant pas couvertes par les autres catégories standardisées de données de passagers, s'agissant là d'un pouvoir discrétionnaire qui n'est pas accordé à l'UIP. Il s'agit par conséquent d'un traitement disproportionné de cette donnée à caractère personnel, dès lors que le traitement des données des passagers doit être limité à ce qui est strictement autorisé par la loi. Ce point de vue rejoint également le récent arrêt de la Cour de Justice de l'Union

[55] Voir l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 *« modifiant diverses dispositions relatives au traitement des données des passagers »*.
[56] Article 37 de la loi PNR. L'UIP fait remarquer qu'il n'y a actuellement qu'avec le Royaume-Uni que des conventions concrètes ont été passées concernant l'échange de données PNR.
[57] Article 37 §3 de la loi PNR.
[58] Réponse de l'UIP du 14 avril 2022.

européenne, selon lequel ce type de données de passagers ne répond pas aux exigences de clarté et de précision[59]. Cela signifie que l'UIP ne peut pas conserver cette information, et doit par conséquent prendre les mesures nécessaires pour que les compagnies aériennes et les agences de voyage ne lui fournissent pas l'adresse IP du système informatique.

Dans sa réponse au projet de rapport, l'UIP fait remarquer qu'elle a dans l'intervalle pris les mesures nécessaires pour que l'UIP ne traite plus l'adresse IP (ni d'autres données qui ne sont pas mentionnées à l'article 9 de la loi PNR). Le COC en prend acte et supprime donc la mesure correctrice proposée dans le projet de rapport.

5. CONCLUSION

33. Dans le cadre du suivi du rapport de contrôle de 2020, le COC constate que l'UIP a dans l'intervalle donné suite aux recommandations dudit rapport. Il ressort par ailleurs des procédures internes de l'UIP que celle-ci prête attention à la protection des données et veille à offrir des garanties additionnelles en vue de la minimalisation des données.

L'enquête menée par l'Organe de contrôle quant à l'efficacité de la banque de données des passagers met clairement au jour un certain nombre de problèmes susceptibles de miner l'efficacité du système PNR. Il arrive notamment que les *matches* (*hits* validés) soient transmises trop tard ou soient reçues trop tard par le service de police intervenant, que les données de passagers transmises ne soient pas toujours exactes, et que moins d'interventions policières soient effectuées en raison de la politique d'action actuelle d'une entité de police donnée.

Cela a d'une part un impact sur l'efficacité de la finalité poursuivie par la banque de données des passagers, à savoir la lutte contre le terrorisme et les formes graves de criminalité. D'autre part, cela conduit dans certains cas à des situations dans lesquelles des personnes font à tort l'objet d'une enquête qui ne les concerne en réalité pas, ou sont à tort interceptées par la douane ou par la GPI à l'aéroport. La cause des problèmes constatés est généralement extérieure à l'UIP. Pour une part, ces problèmes sont en effet également dus à la qualité des données enregistrées dans la Banque de données nationale générale (BNG), une problématique que l'Organe de contrôle a déjà épinglée à plusieurs reprises.

Il est difficile à ce stade d'apporter une réponse objective à la question de savoir si la banque de données des passagers a une plus-value mesurable dans des informations spécifiques. S'il est vrai que l'on pourrait répondre par l'affirmative à cette question en se basant sur le rapport annuel de l'UIP, notamment sur la base des *hits* (générés à partir de profils) et des résultats communiqués à l'UIP par les destinataires des *hits*, il n'est pas possible actuellement de formuler une réponse claire en ce qui concerne l'efficacité de ce système dans le cadre de l'investigation, par la police, des phénomènes de terrorisme et des formes graves de criminalité. Les éléments représentatifs (chiffres) ne sont en effet pas suffisants, principalement en raison de l'absence d'informations concernant l'utilisation des données PNR dans le processus de traitement de l'information ou de l'instruction judiciaire.

Compte tenu des éléments qui précèdent, il convient donc de procéder à une évaluation politique de l'efficacité de la banque de données des passagers. Il y a lieu de renvoyer ici au récent arrêt du 21 juin 2022[60] de la Cour de Justice de l'Union européenne (arrêt de la Cour dans l'affaire C-817/19, *Ligue des droits humains*), dans lequel la Cour indique notamment que les droits fondamentaux exigent que les compétences de traitement prévues par la directive PNR ne peuvent être exercées que dans la mesure où c'est strictement nécessaire. Lorsqu'un État membre ne fait pas face à une menace terroriste qui s'avère réelle et actuelle ou prévisible, le droit de l'Union s'oppose à la législation nationale en vertu de laquelle les données PNR doivent être transmises et traitées pour les déplacements effectués au sein de l'Union européenne en avion et avec d'autres formes de transport. Cet arrêt nécessitera en tout état de cause une révision approfondie de la réglementation belge ainsi que du fonctionnement de l'UIP.

Enfin, l'Organe de contrôle constate que les membres détachés des services de police endossent une double fonction et accomplissent donc aussi des devoirs d'information et d'enquête et établissent des procès-verbaux et/ou des rapports confidentiels. Or, il s'agit là d'un traitement policier qui semble aller plus loin que la compétence du fonctionnaire de police détaché auprès de l'UIP telle qu'elle est strictement réglementée par la loi PNR, et qui doit donc de l'avis du COC être considéré comme problématique d'un point de vue juridique. Le COC appelle donc le législateur à apporter la clarté nécessaire dans la loi PNR, compte tenu de la délimitation des finalités de la directive PNR.

---

[59] Considérant 135 (Cour de Justice de l'Union européenne, 21 juin 2022, C-817/19).
[60] https://curia.europa.eu/juris/document/document.jsf;jsessionid=650151DB421A7F88628FE6238F6052F7?text=&docid=261282&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=5680444.

Approuvé par l'Organe de contrôle de l'information policière le 11 octobre 2022.

Pour l'Organe de contrôle,

Koen Gorissen	Frank Schuermans	Philippe Arnould
Membre-conseiller	Membre-conseiller	Président

Copie électronique :

- à la présidente de la Chambre des Représentants ;
- au président de la Commission Intérieur, Sécurité, Migration et Matières administratives de la Chambre des Représentants
- au ministre de la Justice ;
- au ministre de l'Intérieur ;
- au président du Collège des procureurs généraux ;
- au président de la Commission permanente de la police locale.


CONTROLEORGAAN OP DE POLITIONELE INFORMATIE
ORGANE DE CONTROLE DE L'INFORMATION POLICIERE