Nº 7741

CHAMBRE DES DEPUTES

Session ordinaire 2020-2021

P R O J E T D E L O I

portant modification

1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ;

2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat ; et

3° du Code pénal.

* * *

(Dépôt: le 30.12.2020)

SOMMAIRE:

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre de la Sécurité intérieure et après délibération du Gouvernement en Conseil ;

Arrêtons :

Article unique. – Notre Ministre de la Sécurité intérieure est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi portant modification

1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ;

2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; et

3° du Code pénal.

Biarritz, le 23 décembre 2020

Le Ministre de la Sécurité intérieure,
Henri KOX

HENRI

TEXTE DU PROJET DE LOI

Chapitre 1er – Dispositions modifiant la loi modifiée du 18 juillet 2018 sur la Police grand-ducale

Art. 1. L'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale est remplacé par le texte suivant :

« **Art. 43.** (1) Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'officier ou d'agent de police judiciaire ou d'officier ou d'agent de police administrative ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants :

1° le registre général des personnes physiques créé par la loi du 19 juin 2013 relative à l'identification des personnes physiques et le répertoire général créé par la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ;

2° le fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la Sécurité sociale, à l'exclusion de toutes données relatives à la santé ;

3° le fichier des étrangers exploité pour le compte du Service des étrangers du ministre ayant l'Immigration dans ses attributions ;

4° le fichier des demandeurs d'asile exploité pour le compte du Service des réfugiés du ministre ayant l'Immigration dans ses attributions ;

5° le fichier des demandeurs de visa exploité pour le compte du bureau des passeports, visas et légalisations du ministre ayant les Affaires étrangères dans ses attributions ;

6° le fichier des autorisations d'établissement exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions ;

7° le fichier des titulaires et demandeurs de permis de conduire exploité pour le compte du ministre ayant les Transports dans ses attributions ;

8° le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministre ayant les Transports dans ses attributions ;

9° le fichier des armes prohibées du ministre ayant la Justice dans ses attributions.

(2) Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'officier de police judiciaire ou d'officier de police administrative ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants, s'ils font partie d'une entité de la Police dont les missions justifient cet accès ou figurent sur une liste agrée par le directeur général de la Police après avis du délégué à la protection des données de la Police :

1° le fichier des assujettis à la taxe sur la valeur ajoutée, exploité pour le compte de l'Administration de l'enregistrement et des domaines ;

2° le fichier des sociétés du registre de commerce et des sociétés ;

3° le registre foncier ;

4° le registre des bénéficiaires effectifs ;

5° le registre public des bâtiments de plaisance battant pavillon luxembourgeois ;

6° le système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg ;

7° le registre des fiducies et des trusts.

(3) Les membres du cadre civil de la Police, nommément désignés par le ministre sur proposition du directeur général de la Police grand-ducale, après avis du délégué à la protection des données de la Police, peuvent avoir accès aux fichiers prévus aux paragraphes (1) et (2) en fonction de leurs attributions spécifiques de support d'un officier ou agent de police judiciaire ou d'un officier ou agent de police administrative ou à des fins administratives.

(4) Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'agent de police judiciaire ou d'agent de police administrative nommément désignés par le directeur général de la Police grand-ducale, après avis du délégué à la protection des données de la Police, peuvent avoir accès aux fichiers prévus aux paragraphes (2).

(5) Les données à caractère personnel des fichiers accessibles en vertu des paragraphes (1) et (2) sont déterminées par règlement grand-ducal.

(6) Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que :

1° les membres de la Police visés aux paragraphes (1), (2) et (3) ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel ; et

2° les informations relatives aux membres de la Police ayant procédé à la consultation ainsi que les informations consultées, le motif de la consultation, ainsi que la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de cinq ans.

(7) Nonobstant les droits d'accès prévus aux paragraphes (1) à (4), les données à caractère personnel consultées doivent avoir un lien direct avec les motifs de consultation. Seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées.

(8) L'autorité de contrôle prévue à l'article 2, paragraphe 1er, point 15), lettre a), de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale contrôle et surveille le respect des conditions d'accès prévues par le présent article. Le rapport à transmettre au ministre ayant la protection des données dans ses attributions, en exécution de l'article 10 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercée au titre du présent article. »

Art. 2. A la suite de l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, il est inséré un article 43-1 nouveau, qui prend la teneur suivante :

« **Art. 43-1.** (1) Sans préjudice de dispositions légales spécifiques, le présent article 43-1 s'applique à tous les fichiers que la Police gère en tant que responsable du traitement, conformément à l'article 1er de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

(2) Les fichiers de la Police peuvent contenir des données à caractère personnel relevant des catégories particulières prévues par l'article 9 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale dans la mesure où ces catégories particulières de données sont pertinentes et essentielles à l'aide de l'identification d'une personne, pour comprendre le contexte décrit dans un rapport ou procès-verbal établi par la Police et pour apprécier correctement les faits qui peuvent donner lieu à une infraction pénale ou à une mesure de police administrative au sens de la section 1ière du chapitre 2 de la présente loi ou en vertu d'une autre mission dont la Police est investie par la loi. Les données de ce type ont toujours un rapport avec d'autres données relatives à la personne concernée.

(3) La Police détermine des profils et des modalités d'accès et de traitement de données à caractère personnel sur la base :

1° du détail des informations concernées. La Police met en œuvre des règles spécifiques pour l'accès à ses rapports, procès-verbaux et autres pièces ;

2° du type du traitement de données, tels qu'une collecte, une modification, une consultation, une communication, un effacement ou une transmission de données ;

3° de l'appartenance à un service déterminé ou d'une unité au sein de la Police et de la fonction du membre de la Police ;

4° du motif d'accès. Si le motif d'accès ne découle pas incontestablement de l'affectation de l'agent au sein d'un service ou d'une unité de la Police, le motif d'accès doit indiquer la raison précise de la consultation. La Police détermine des motifs d'accès spécifiques selon le type de mission légale de la Police dans le cadre de laquelle un traitement de données est requis ;

5° de l'état de validation des données traitées ;

6° des règles spécifiques pour les données relatives à des mineurs qui prévoient que les rapports, procès-verbaux et autres pièces établis par la Police par rapport à un mineur ne peuvent être accédés que par :

a) les membres de la section « protection de la jeunesse » au sein du Service de police judiciaire ;

b) les officiers et agents de police judiciaire qui sont chargés d'une enquête par rapport au mineur concerné ou suite à une demande du service central d'assistance sociale (SCAS) du Parquet Général.

Dans le cas d'une demande de consultation d'un fichier par une personne autre que celle qui l'effectue, les journaux du fichier font mention de l'identité de la personne à l'origine de la demande et du motif de cette demande.

(4) La durée de conservation des données est définie par le responsable du traitement et ne sera en aucun cas supérieure à celles qui sont applicables au fichier central, sauf si une disposition légale spécifique prévoit une durée plus longue.

(5) Les données de journalisation collectées conformément à l'article 24 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont conservées pendant un délai de cinq ans. «

Art. 3. A la suite de l'article 43-1 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, il est inséré un article 43-2 nouveau, qui prend la teneur suivante :

« **Art. 43-2.** (1) Dans le fichier central, la Police peut traiter les données à caractère personnel et informations relatives aux personnes qui ont fait l'objet d'un procès-verbal ou rapport dans le cadre de l'exécution d'une mission de police judiciaire, d'une mission de police administrative ou de toute autre mission dont la Police est investie par la loi.

Le fichier central comprend une partie active et une partie passive. La partie active contient les données auxquelles les membres de la Police ont besoin d'accéder dans le cadre de leurs missions légales conformément aux délais de conservations prévus aux paragraphes 9, 10, 11, 13 et 14. Après avoir atteint la durée de conservation maximale dans la partie active, les données collectées dans le cadre de l'exécution d'une mission de police judiciaire sont transférées dans la partie passive, à laquelle l'accès n'est justifié que pour les finalités prévues au paragraphe 19.

Le fichier central ne comporte pas les données relatives à des personnes qui ont commis une contravention si une loi spéciale permet d'arrêter les poursuites pénales par le paiement d'un avertissement taxé et que la personne concernée s'est acquittée de l'avertissement taxé dans le délai prévu par la loi.

(2) Les données à caractère personnel et informations sont traitées dans le fichier central pour les finalités suivantes :

1° la vérification des antécédents d'une personne dans le cadre d'une mission de police judiciaire, de police administrative ou dans le cadre d'une autre mission légale de la Police ;

2° l'appui aux enquêtes judiciaires par le biais d'analyses criminelles opérationnelles à la demande d'une autorité judiciaire ;

3° l'appui à la définition et à la réalisation de la politique de sécurité intérieure par le biais d'analyses criminelles stratégiques ;

4° l'exploitation des informations à des fins de recherches statistiques ;

5° l'identification des membres de la Police en charge du dossier.

(3) Les catégories de personnes concernées dont les données sont traitées dans le fichier central aux fins de police administrative et de toute autre mission dont la Police est investie par la loi, sont

les personnes ayant fait l'objet d'une mesure de police ou ayant été citées dans un rapport établi par la Police dans le cadre de l'exécution de ses missions. Ces catégories comprennent :

1° les personnes ayant fait l'objet d'une mesure de police administrative prise par la Police au sens de la section 1ière du chapitre 2 de la présente loi ou sur base d'une loi spéciale ;

2° les personnes signalées ou recherchées par la Police afin que la Police puisse accomplir ses missions au sens de l'article 7 de la présente loi ;

3° les membres de la Police en charge du dossier.

(4) Les catégories de personnes dont les données sont traitées dans le fichier central aux fins de police judiciaire sont les suivantes :

1° les personnes suspectées d'avoir participé à une infraction pénale ;

2° les personnes reconnues coupables d'une infraction pénale ;

3° les personnes décédées de manière suspecte ;

4° les personnes disparues ;

5° les personnes signalées ou recherchées par la Police ;

6° les personnes évadées ou qui ont tenté de s'évader ;

7° les personnes qui exécutent une peine ;

8° les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;

9° les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures ;

10° les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale, ainsi que les contacts ou associés qui sont suspectés d'avoir l'intention de participer à ces infractions ou d'en avoir connaissance, ainsi que les personnes qui peuvent fournir des informations sur ces infractions pénales ;

11° les membres de la Police en charge du dossier.

Les personnes visées au point 10° ne peuvent faire l'objet d'une inscription dans le fichier central que :

1° par les officiers de police judiciaire du Service de police judiciaire dans les matières qui relèvent des attributions de la section à laquelle ils sont affectés ;

2° si la fiabilité de la source et de l'information est évaluée suivant un code d'évaluation préalablement défini qui tient compte de la pertinence de la source et de l'information fournie dans le contexte de l'évolution de la criminalité et des phénomènes criminels pertinents ; et

3° avec l'accord du procureur général d'Etat ou du membre de son parquet désigné à cet effet si ces données concernent un mineur.

(5) Une consultation du fichier central pour un motif autre qu'un motif de police judiciaire ne donne pas accès aux données à caractère personnel des personnes prévues à l'article 43-2, paragraphe (4), points 8°, 9° et 10°, sauf pour les consultations administratives qui relèvent de la police des étrangers qui donnent accès aux points 8° et 9°.

Une consultation du fichier central pour un motif de police judiciaire ne donne pas accès aux données à caractère personnel des personnes prévues à l'article 43-2, paragraphe (4), alinéa 1er, point 10° à l'agent consultant, mais génère un avertissement auprès des officiers de police judiciaire en charge de l'information. Il appartient aux agents en charge de l'information d'évaluer l'utilité de prendre contact avec l'agent consultant.

Par dérogation à l'alinéa précédent, les officiers et les agents de police judiciaire du Service de police judiciaire ont accès direct à ces données, sauf si les agents qui sont en charge de l'information ont limité l'accès à une ou plusieurs sections du Service de police judiciaire.

Les agents en charge de l'information peuvent autoriser l'accès direct aux informations à l'égard des personnes auxquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale. Dans ce cas, ces informations sont traitées comme celles qui relèvent des catégories prévues au paragraphe (4), alinéa 1er, point 1°.

(6) Pour l'exercice de leurs fonctions, un accès direct au fichier central peut être accordé par le responsable du traitement aux fonctionnaires de l'Administration des douanes et accises ayant la qualité d'officier de police judiciaire et nommément désignés par le directeur de l'Administration des douanes et accises.

Pour l'exercice de leurs missions prévues aux articles 4, 8 et 9 de la loi modifiée du 18 juillet 2018 sur l'Inspection générale de la Police, un accès direct au fichier central peut être accordé par le responsable du traitement à l'Inspecteur général de la Police, à l'Inspecteur général adjoint de la Police et aux membres du cadre policier de l'Inspection générale de la Police.

(7) Dans le respect des règles d'accès déterminées en vertu de l'article 43-1, paragraphe (3) de la présente loi, le fichier central permet aux officiers et agents de police judiciaire et de police administrative, ainsi qu'au membres du personnel civil nommément désignés par le responsable du traitement, de déterminer si une personne y figure. Elle permet également à visionner les informations et données à caractère personnel principales par rapport à cette personne et, le cas échéant, un résumé sommaire de faits dans lesquels la personne est impliquée. Les procès-verbaux et rapports dont la personne fait l'objet sont également accessibles en fonction des droits d'accès et des motifs de la consultation.

Les informations et données à caractère personnel principales par rapport aux personnes visées aux paragraphes (3) et (4) peuvent contenir les données suivantes si elles sont disponibles pour les personnes physiques :

1° le(s) nom(s), prénom(s), alias et surnoms ;

2° la date et le lieu de naissance ;

3° la ou les nationalités ou le statut d'apatride ;

4° l'état civil ;

5° la date de décès ;

6° le numéro d'identification national ou, le cas échéant, un numéro équivalent ;

7° le domicile, la résidence habituelle ou la dernière adresse connue ;

8° le numéro de la carte d'identité et/ou du passeport ou de tout autre document officiel ;

9° le numéro du téléphone et les données y afférentes et, le cas échéant, une adresse électronique ;

10° le signalement descriptif, comprenant les signes corporels inaltérables permettant d'identifier la personne, y compris les photographies et, le cas échéant, les empreintes digitales.

Dans le cas d'une personne morale, les informations et données à caractère personnel principales peuvent contenir les données suivantes si elles sont disponibles :

1° la dénomination sociale et, le cas échéant, la dénomination commerciale si elle est différente de la dénomination sociale ;

2° le(s) nom(s), prénom(s), alias et surnoms des dirigeants et des bénéficiaires économiques ainsi que leur date et lieu de naissance et leur numéro d'identification national ou, le cas échéant, un numéro équivalent ;

3° la date et le lieu de constitution ;

4° l'adresse du siège social et les adresses d'exploitation ;

5° le numéro du téléphone et les données y afférentes et, le cas échéant, une adresse électronique.

(8) Les données à caractère personnel et les informations prévues aux paragraphes (3) et (4) sont transmises au fichier central si l'enquête est terminée, ou si l'autorité judiciaire compétente a autorisé la transmission conformément à la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière.

(9) En présence d'une décision de condamnation coulée en force de chose jugée, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour crime ou délit adressés aux autorités judiciaires sont transférées dans la partie passive du fichier central dès que la Police est informée que la décision de condamnation est supprimée du casier judiciaire de toutes les personnes condamnées.

Si la réhabilitation ne concerne pas toutes les personnes impliquées dans la poursuite pénale de l'affaire visée, les informations et données à caractère personnel de la personne réhabilitée sont maintenues dans la partie active. Dans ce cas, la personne réhabilitée dans l'affaire visée ne peut plus être recherchée dans la partie active par le biais de ses données à caractère personnel à partir de la suppression de la condamnation du casier judiciaire.

Dès qu'une condamnation est prononcée dans une affaire, les victimes et témoins ne peuvent plus être recherchés dans la partie active par le biais de leurs données à caractère personnel, sauf si une disjonction des poursuites a été prononcée dans l'affaire visée et que la recherche de personnes suspectées d'avoir participé à l'infraction continue.

(10) En présence d'une décision d'acquittement coulée en force de chose jugée, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour crime ou délit adressés aux autorités judiciaires sont transférées dans la partie passive du fichier central dès que la Police est informée de la décision d'acquittement, sauf si le Procureur d'Etat ordonne leur maintien.

Si l'acquittement ne concerne pas toutes les personnes impliquées dans la poursuite pénale de l'affaire visée ou si après l'acquittement d'un prévenu l'enquête est reprise pour rechercher l'auteur de l'infraction, les informations et données à caractère personnel de la personne acquittée sont maintenues dans la partie active. Dans ce cas, la personne acquittée dans l'affaire visée ne peut plus être recherchée dans la partie active par le biais de ses données à caractère personnel, sauf si la personne concernée a fait l'objet d'une audition comme témoin dans une phase initiale de l'enquête, dans quel cas elle reste liée à l'affaire sous ces statuts respectifs.

Si l'enquête est reprise suite à un acquittement ou si l'enquête continue suite à une disjonction des poursuites, les données relatives aux victimes et témoins sont maintenues dans la partie active.

(11) En l'absence de décision coulée en force de chose jugée d'une juridiction de jugement, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour crime ou délit adressés aux autorités judiciaires, sont conservées dans la partie active du fichier central jusqu'à ce que le dossier relatif à la poursuite pénale soit archivé au sein du traitement, dit chaîne pénale du ministère public. Les informations et données à caractère personnel sont transférées dans la partie passive du fichier central dès que la Police est informée de l'archivage au sein du traitement, dit chaîne pénale, du ministère public.

(12) Les décisions de condamnation, d'acquittement, de non-lieu ou de classement sans suites sont mentionnées dans le fichier central.

(13) Le procureur d'Etat peut à tout moment, d'office ou à la demande de la personne concernée, soit ordonner le transfert des informations, données à caractère personnel, procès-verbaux ou rapports relevant d'une mission de police judiciaire dans la partie passive du fichier central, soit ordonner que la personne concernée ne puisse plus être recherchée par le biais des données à caractère personnel. La décision est communiquée par écrit à la Police et fait l'objet d'une mention dans le dossier en question. Le procureur d'État avise la personne concernée des suites qu'il convient de donner aux demandes qui lui sont adressées.

Les décisions du Procureur d'Etat visées à l'alinéa précédent sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé ou si des raisons objectives ne justifient plus leur maintien.

Les décisions du procureur d'Etat sont susceptibles de recours devant le Président du tribunal d'arrondissement compétent en la matière.

(14) Par dérogation aux paragraphes 9, 10 et 11, les informations et données à caractère personnel sont transférées dans la partie passive après vingt ans pour les rapports rédigés dans le contexte d'une demande d'entraide judiciaire internationale.

Les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des documents qui relèvent de la coopération policière internationale ou dans des rapports aux autorités judiciaires qui n'ont pas comme objet la constatation d'une infraction pénale sont transférées dans la partie passive ensemble avec les procès-verbaux ou rapports élaborés dans le cadre de l'enquête à laquelle ils se rapportent. Si ces rapports ne concernent pas une enquête en

cours ou une infraction déterminée, le délai de conservation prévu au paragraphe 15, alinéa 1er est applicable.

Les informations et données à caractère personnel contenues dans le fichier central qui relèvent des personnes visées à l'article 43-2, paragraphe (4), alinéa 1er, point 10° sont transférées dans la partie passive un an après leur enregistrement dans la partie active du fichier central. Ce délai peut être prolongé d'une année supplémentaire sur décision motivée de l'officier de police judiciaire en charge de l'information dans le fichier central. Si l'information se révèle être inexacte, elle est immédiatement supprimée. Seul l'officier de police judiciaire en charge de l'information peut la supprimer.

(15) Les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des rapports rédigés dans le cadre d'une mission de police administrative ou dans le cadre d'une mission administrative dont la Police est investie par la loi, sont supprimées au plus tard après une période de dix ans après leur enregistrement dans le fichier central. La Police peut arrêter des délais de conservation plus courts par type de rapport au sens de ce paragraphe, auquel cas elle tient un relevé dans lequel les délais spécifiques sont indiqués.

Les informations et données à caractère personnel contenues dans le fichier central relatives à des personnes mineures en fugue sont effacées du fichier central lorsque la personne a atteint l'âge de dix-huit ans.

(16) Les informations et données à caractère personnel contenues dans la partie passive du fichier central, et le cas échéant dans la partie passive des fichiers particuliers établis conformément à l'article 43-1, peuvent être retransmises dans la partie active pour les raisons suivantes :

1° les enquêtes sont reprises pour des infractions pénales qui ne sont pas encore prescrites ;

2° il s'agit d'enquêtes relatives à des faits dénoncés à des autorités judiciaires d'autres États ;

3° il s'agit de faits qui relèvent d'une décision d'enquête européenne ou d'une commission rogatoire internationale.

Une retransmission dans la partie active du traitement, dit chaîne pénale, du ministère public donne lieu à une retransmission dans la partie active du fichier central. Les informations et données à caractère personnel sont de nouveau transférées dans la partie passive du fichier central dès que la Police est informée de l'archivage au sein du traitement, dit chaîne pénale, du ministère public.

(17) Sans préjudice des dispositions relatives à l'archivage pour des raisons historiques, les informations et données à caractère personnel sont supprimées au plus tard trente ans après leur transfert dans la partie passive.

Par dérogation à l'alinéa qui précède, les informations et données à caractère personnel contenues dans le fichier central qui relèvent des personnes visées à l'article 43-2, paragraphe (4), alinéa 1er, point 10° sont supprimées trois ans après leur transfert dans la partie passive.

Par dérogation à l'alinéa 1er, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour contraventions adressés aux autorités judiciaires, sont supprimées cinq ans après l'établissement du procès-verbal ou du rapport.

Les autorités judiciaires compétentes peuvent faire prolonger la durée de conservation dans la partie passive en raison d'une demande de révision en cours. La décision est communiquée par écrit à la Police et fait l'objet d'une mention dans le dossier en question.

(18) Au plus tard au moment du transfert dans la partie passive du fichier central des informations et données à caractère personnel relevant d'une mission de police judiciaire, les informations et données à caractère personnel en question qui se trouvent dans d'autres fichiers doivent être supprimées dans ceux-ci, sauf si ces fichiers sont régis par une disposition légale spécifique qui prévoit une durée de conservation différente.

Par dérogation à l'alinéa précédent, les informations et données à caractère personnel contenues dans d'autres fichiers dans un format qui ne peut pas être géré par le fichier central peuvent être archivées dans le fichier particulier s'il dispose d'une possibilité d'archivage. Les durées d'archivage et les conditions d'accès sont les mêmes que celles prévues pour la partie passive du fichier central.

Par dérogation à l'alinéa 1er, l'obligation de suppression des informations et données à caractère personnel contenues dans d'autres fichiers au moment du transfert des informations dans la partie passive du fichier central ne s'applique pas aux informations et données à caractère personnel relatives à des traces prélevées dans le cadre d'enquêtes où les auteurs des faits sont restés inconnus. Les durées de conservation sont les mêmes que celles prévues pour la partie passive du fichier central.

(19) L'accès aux informations et données à caractère personnel contenues dans la partie passive du fichier central, et le cas échéant dans la partie passive des fichiers particuliers établis conformément à l'article 43-1, peut être effectué pour les seules finalités suivantes :

1° la prise de connaissance des informations dans le cadre d'une enquête en cours relative à un crime ou un délit ;

2° la prise de connaissance des informations dans le cadre d'une demande en révision conformément aux articles 443 et suivants du Code de procédure pénale.

La consultation des informations et données à caractère personnel contenues dans la partie passive du fichier central pour une de ces finalités n'est possible qu'avec l'accord du procureur général d'Etat ou des membres de son parquet désignés à cet effet ou, pour la finalité sous 1°, sur demande du juge d'instruction en charge de l'instruction préparatoire.

Le procureur général d'État peut autoriser l'accès aux informations et données à caractère personnel contenues dans la partie passive du fichier central à des officiers et agents de police judiciaire nommément désignées du Service de police judiciaire ou aux membres de certaines subdivisions du Service de police judiciaire pendant une période maximale de cinq ans renouvelable.

Art. 4. A la suite de l'article 43-2 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, il est inséré un article 43-3 nouveau, qui prend la teneur suivante :

« **Art. 43-3.** La Police grand-ducale a la qualité de responsable du traitement des traitements de données à caractère personnel effectués par la Police. »

Chapitre 2 – Autres dispositions modificatives

Art. 5. À l'article 10, paragraphe 2, de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, le point h) est supprimé.

Art. 6. Le Code pénal est modifié comme suit :

1° Au titre de la « Section VII – De certaines infractions en matière informatique » du Code pénal sont ajoutés les mots « et de systèmes de traitement ou de transmission automatisé » :

« Section VII – De certaines infractions en matière informatique **et de systèmes de traitement ou de transmission de données** »

2° A l'article 509-1 du Code pénal sont ajoutés les mots « ou non-automatisé » après les mots « d'un système de traitement ou de transmission automatisé » et à la suite de l'alinéa 1er est inséré un nouvel alinéa 2 :

« **Art. 509-1.** Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé **ou non-automatisé** de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Sera puni des mêmes peines, quiconque, disposant d'une autorisation d'accès à tout ou partie d'un système de traitement ou de transmission automatisé ou non-automatisé de données à caractère personnel, y effectue un traitement de données à caractère personnel pour des finalités autres que celles pour lesquelles l'autorisation d'accès a été accordée, y inclus le fait de porter à la connaissance d'un tiers non autorisé les données à caractère personnel ainsi obtenues.

Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros. »

3° Aux articles 509-2 et 509-3 du Code pénal, sont ajoutés les termes « **ou non-automatisé** » après les mots « d'un système de traitement ou de transmission automatisé. »

Chapitre 3 – Dispositions transitoires

Art. 7. Les fichiers autres que le fichier central de la Police établis avant l'entrée en vigueur de la présente loi sont mis en conformité avec l'article 43-1 de la présente loi au plus tard le 6 mai 2023.

Par dérogation à l'alinéa 1er, lorsque cela exige des efforts disproportionnés et l'intervention de ressources externes, les fichiers autres que le fichier central peuvent être mis en conformité avec l'article 43-1 de la présente loi jusqu'au 6 mai 2026.

Le fichier central exploité par la Police avant l'entrée en vigueur de la présente loi restera accessible aux officiers et agents de police judiciaire pendant une période d'une année après l'entrée en vigueur de la présente loi.

Pendant cette période, à chaque nouvelle inscription dans le fichier central au sens de la présente loi, les informations, procès-verbaux et rapports pertinents relatifs à ces personnes et contenus dans l'ancien fichier central sont supprimés dans celui-ci et seront repris dans le nouveau fichier central, si les conditions légales pour une conservation dans la partie active ou passive du nouveau fichier central sont toujours remplies.

Au-delà de ce délai, il restera accessible aux seuls membres du centre d'intervention national et aux membres du service fichier central pendant une période supplémentaire de trois ans.

Cinq ans après l'entrée en vigueur de la présente loi, toutes les informations et données à caractère personnel contenues dans la partie active de l'ancien fichier central seront transférées dans la partie passive.

La partie passive de l'ancien fichier central restera accessible suivant les mêmes modalités que celles prévues pour la partie passive du fichier central tel que prévu à l'article 43-2.

Chapitre 4 – Disposition finale

Art. 8. La présente loi entre en vigueur le 1er jour du sixième mois après la publication au Journal officiel du Grand-Duché de Luxembourg, à l'exception des articles 1, 4, 5, 6, et 7 qui entrent en vigueur conformément au droit commun.

*

EXPOSE DES MOTIFS

1. Les fichiers de la Police grand-ducale

Le projet de loi sous rubrique a pour objet d'encadrer les traitements des données à caractère personnel effectués dans les fichiers de la Police grand-ducale, et plus précisément dans le fichier central. Il vise à adresser les critiques en matière de protection des données qui ont été soulevées par rapport aux fichiers de la Police, et plus particulièrement par rapport au fichier central en été 2019.

Dans ce contexte, le ministre de la Sécurité intérieure avait sollicité la Commission nationale pour la protection des données (CNPD) pour rendre un avis au sujet du fichier central, ainsi que l'Inspection générale de la Police (IGP) pour élaborer une étude sur tous les fichiers de la Police. Les recommandations émises par la CNPD et l'IGP ont fait ressortir la nécessité d'un encadrement légal plus strict, notamment dans les domaines des droits d'accès, des délais de conservation ainsi que des précisions relatives aux finalités du fichier central.

Alors que la base légale des fichiers de la Police n'est pas mise en question, la CNPD a conclu dans son avis du 13 septembre 2019 que

> « *la loi sur la Police devrait être complétée de dispositions précisant, entre autres, le principe et les finalités spécifiques des fichiers opérés par la Police grand-ducale pour les besoins d'exécution de ses missions, les délais de conservation des données ou les critères applicables pour déterminer les durées de conservation des données, ainsi que les autres aspects essentiels des traitements de données opérés par la Police.* »

A la suite des débats politiques relatifs aux fichiers de la Police, un consensus a émargé d'élaborer un projet de loi qui encadre de manière spécifique le traitement de données à caractère personnel dans les fichiers de la Police, et notamment dans le fichier central, et qui offre des garanties supplémentaires à celles prévues par la légalisation relative à la protection des données.

A. *Les fichiers de la Police grand-ducale : la situation avant la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale*

Au Luxembourg, les traitements des données à caractère personnel par la Police sont encadrés par la législation générale en matière de protection de données. Actuellement, la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, ci-après dénommée « la loi du 1er août 2018 », sert de fondement légal aux traitements de données à caractère personnel effectués par la Police grand-ducale. Avant l'entrée en vigueur de la loi précitée, le traitement des données à caractère personnel fut régi par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

L'article 17 de la loi modifiée du 2 août 2002 stipulait que « *les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises* » doivent faire l'objet d'un règlement grand-ducal.

Sur base de cette disposition, certains fichiers de la Police ont été encadrés par voie de règlements grand-ducaux spécifiques, comme par exemple le fichier des données relatives aux avertissements taxés, tel que prévu par le règlement grand-ducal modifié du 21 décembre 2004 portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière ou le fichier des données résultant du système de contrôle et de sanction automatisés, tel que prévu par le règlement grand-ducal modifié du 7 août 2015 autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de contrôle et de sanction automatisés.

Certains fichiers de la Police d'ordre plus général trouvaient leur base légale dans le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale qui était pris en vertu de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques. Le règlement grand-ducal précité servait de base légale au fichier central tel qu'il existe dans son état actuel. Ce dernier dispose d'une fonction de recherche permettant sur la base du nom ou la date de naissance ou du numéro de dossier pour les procès-verbaux et rapports de vérifier si une personne y figure. Après dix ans, les documents et données sont archivés et ne sont par conséquent plus accessibles aux agents, sauf sur accord du procureur général d'Etat ou du membre de son parquet désigné à cet effet.

Malgré l'abrogation de la loi modifiée du 31 mars 1979 précitée par la loi modifiée du 2 août 2002 précitée, l'article 44 de cette dernière permettait de prolonger des règlements grand-ducaux pris en vertu de la loi modifiée du 31 mars 1979. Ainsi le règlement grand-ducal du 2 octobre 1992 précité fut prolongé à plusieurs reprises et pour la dernière fois par le règlement grand-ducal du 23 décembre 2016 reconduisant les fichiers visés jusqu'au 1er juin 2018, donc juste avant l'entrée en vigueur de la loi du 1er août 2018.

B. *Les fichiers de la Police grand-ducale : la situation suite à la loi du 1er août 2018*

La loi du 1er août 2018 transpose en droit luxembourgeois la directive (UE) 2016/680[1]. Elle s'applique à tous les traitements de données à caractère personnel effectués par la Police en matière pénale

1 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.

ainsi qu'en matière de sécurité nationale. Elle s'applique également à l'exécution de missions à d'autres fins pour autant que celles-ci soient prévues par des lois spéciales.

La loi du 1er août 2018 constitue le fondement légal pour le fichier central ainsi que pour les autres fichiers créés, gérés et mis à jour par la Police, tel que confirmé par la CNPD dans son avis du 13 septembre 2019 relatif au fichier central :

> « *En d'autres termes, même si cette loi n'est pas spécifiquement dédiée à la gestion et l'exploitation du fichier central, elle encadre néanmoins les traitements dudit fichier utilisé par la Police dans le cadre des missions qui lui sont conférées par la loi du 18 juillet 2018 sur la Police grand-ducale.* »

Ainsi la loi du 1er août 2018 permet à la Police, en tant que responsable du traitement, de traiter des données à caractère personnel dans le cadre de ses missions légales et de prendre des décisions relatives à la création, le maintien et la modification de ses fichiers. Suite à l'entrée en vigueur de la loi du 1er août 2018, la Police continue ses travaux de révision et rationalisation de ses fichiers, un exercice qu'elle avait déjà entamé bien avant.

C. *L'encadrement complémentaire des fichiers de la Police grand-ducale : un équilibre entre le renforcement des garanties supplémentaires en matière de vie privée et la flexibilité requise pour un travail policier efficace*

Dans le cadre des débats politiques relatifs aux fichiers de la Police, la question s'est posée si et dans quelle mesure cette responsabilité de la Police devrait être davantage encadrée et complétée par des dispositions plus spécifiques. D'un point de vue juridique, un tel encadrement complémentaire n'est pas indispensable, toutefois l'article 1.3 de la directive (UE) 2016/680 permet explicitement « *de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes* ».

Suite à une analyse comparative de la législation des pays limitrophes, il s'avère que tous ces pays disposent d'une législation spécifique en matière de bases de données de la police. A cet égard, il convient toutefois de préciser que ces règles furent souvent inscrites dans la législation relative à la police et/ou relative à la procédure pénale bien avant la transposition nationale de la directive (UE) 2016/680, tel qu'est le cas en Belgique et en France. Ces pays ont maintenu leur législation en vigueur, moyennant quelques adaptations, suite à leur transposition de la directive (UE) 2016/680.

Compte tenu de l'existence d'une législation spécifique dans les pays limitrophes et des recommandations de l'IGP et de la CNPD, il est opportun d'encadrer plus spécifiquement les accès des membres de la Police aux différents fichiers ainsi que les délais de conservation des données et, quant au fichier central, les finalités de celui-ci, ainsi que les catégories de personnes et des types de données qui peuvent y figurent. Les dispositions proposées dans le présent projet de loi sont complémentaires à celles de la loi du 1er août 2018.

Au niveau de la structuration des règles complémentaires, le projet de loi s'inspire partiellement de la législation belge, et notamment de la loi du 5 août 1992 sur la fonction de police, dont l'article 44 contient certaines règles communes à tous les fichiers de la police belge. En outre, elle réglemente de manière plus spécifique la « banque de données nationale générale », une base de données qui présente une certaine similarité avec le fichier central luxembourgeois. Les autres fichiers de la police belge ne sont pas spécifiquement réglementés de manière individuelle, mais le dispositif législatif belge divise les fichiers en plusieurs « catégories » de base de données (bases de données « de base », « spécifiques », « techniques » et bases de données « communes » avec d'autres autorités nationales).

Le présent projet de loi suit partiellement la même logique et vise à déterminer un cadre commun à tous les fichiers de la Police et à réglementer plus spécifiquement le fichier central. Concernant les « fichiers particuliers », qui désignent tous les fichiers autres que le fichier central, il incombe à la Police d'en définir les éléments-clé, tout en respectant les règles communes applicables à tous les fichiers de la Police. Un tel système, qui permet à la Police de régler certains aspects par voie interne et de garantir ainsi une efficacité des actions policières rejoint l'idée de la responsabilisation du responsable du traitement, laquelle sous-tend la directive (UE) 2016/680 et la loi de transposition du 1er août 2018.

A titre d'exemple, l'article 4 de la loi du 1er août 2018 permet explicitement au responsable du traitement de régler les délais de conservation en interne. Même si le présent projet de loi encadre davantage les principes des délais de conservation et que ceux-ci seront définis plus en détail pour le fichier central, l'article 4 précité démontre que cette approche qui consiste à laisser une latitude à la Police pour adopter des dispositions complémentaires est parfaitement licite et conforme à la législation en matière de protection des données.

L'approche poursuivie implique également qu'il n'est pas nécessaire d'adopter une loi spécifique pour chaque traitement de données à caractère personnel effectué par la Police, alors que la loi du 1er août 2018 suffit en elle-même comme base légale pour l'ensemble des fichiers de la Police. Le présent projet de loi n'est ainsi pas à considérer comme un changement de ce paradigme.

Concernant les dispositions relatives aux délais de conservation des données à caractère personnel dans le fichier central, les auteurs du projet de loi se sont inspirés de la législation française, et plus particulièrement des articles 230-6 à 230-11 du Code de procédure pénale français relatifs au traitement d'antécédents judiciaires (TAJ). Ces derniers prévoient un certain nombre de règles relatives à la conservation et effacement des données, l'apposition d'une mention ainsi que les prérogatives des autorités judiciaires dans le cadre des fichiers de la Police.

Il convient de préciser que les auteurs du projet de loi ont veillé à ne pas régler des points qui sont couverts à suffisance par la loi du 1er août 2018 ou par d'autres dispositions spécifiques. Ainsi, le projet de loi ne traite pas certains sujets, tels que les droits des personnes concernées, qui sont régis en détail par les dispositions de la loi du 1er août 2018. Un autre exemple est l'article 3, paragraphe 2 de la loi précitée, qui permet explicitement à la Police de traiter des données collectées dans un fichier particulier pour une finalité déterminée, à une autre finalité, et représente ainsi une base légale suffisante pour une interconnexion éventuelle entre les différents fichiers, ou pour une consultation parallèle de plusieurs fichiers au sein de la Police.

La loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière, quant à elle, continue de régir les échanges de données entre différentes entités étatiques.

2. L'accès de la Police aux fichiers d'autres administrations

Les auteurs du projet de loi ont profité de l'occasion pour adapter également l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. Cette disposition prévoit un accès direct pour la Police à certains fichiers d'autres administrations. L'adaptation envisagée a pour but d'adapter la liste des fichiers déjà accessibles à la Police et de mieux encadrer leur accès par la Police.

3. Sanctions pénales

Les auteurs du projet de loi proposent une modification des articles 509-1 et suivants du Code pénal, afin de tenir compte des détournements de finalités des droits d'accès qu'une personne dispose dans le cadre de ses activités.

*

COMMENTAIRE DES ARTICLES

Ad article 1er

Jusqu'à présent, l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale se limitait à accorder des accès aux fins de police judiciaire ou administrative. Toutefois, la Police est également en charge de missions légales qui ne rentrent ni dans l'une, ni dans l'autre catégorie. C'est par exemple le cas en matière des objets trouvés ou de la police des étrangers. Par ailleurs, certains membres de la Police ont besoin d'un accès à certaines banques de données à des fins purement administratives, par exemple, dans le cadre des ressources humaines.

Les fichiers prévus au paragraphe (1) sont ceux auxquels notamment tous les officiers et agents de police judiciaire dans des fonctions opérationnelles ont besoin de pouvoir accéder pour l'accomplissement de leurs missions ordinaires.

Les fichiers repris au paragraphe (2) sont des fichiers spécifiques auxquels seulement certains membres de la Police ont un besoin d'accès. Une première condition est la qualité d'officier de police judiciaire ou d'officier de police administrative, et une deuxième condition est d'être membre d'une entité de la Police pour laquelle l'accès se justifie, ou bien de figurer sur une liste nominative. Dans les deux cas la décision appartient au responsable du traitement.

L'accès aux registres prévus aux points 3, 4, 6 et 7 est déjà prévu dans des lois ou règlements grand-ducaux relatifs à ces fichiers. Pour des raisons de transparence, il est cependant utile de maintenir ces dispositions en place.

Il convient de préciser que le principe de l'accès à d'autres fichiers en vertu de la législation ou d'autres règles applicables qui les encadrent et, en l'absence de telles règles, en vertu du RGPD, reste d'application pour la Police, même si ces fichiers ne sont pas énumérés à l'article 43 de la loi sur la Police. Alors que le RGPD n'oblige plus de disposer d'une base légale ou réglementaire spécifique pour l'accès aux données ou pour le transfert de ces données vers une autre administration, il appartient à chaque responsable du traitement d'effectuer les traitements qui remplissent les critères de licéité en fonction de ses missions et attributions.

Le paragraphe (3) prévoit un accès aux fichiers aux paragraphes (1) et (2) pour les membres du cadre civil qui figurent sur une liste nominative. Il reprend en principe une disposition prévue dans le texte initial mais cette dernière était formulée de manière inadéquate, alors que la phrase relative au personnel civil se référait uniquement aux missions de police judiciaire de de police administrative. Or, le personnel civil n'est pas compétent pour effectuer de telles missions et ne peut que fournir une tâche de support, une précision qui est apportée par le paragraphe 3.

Le principe d'entendre l'avis du délégué à la protection des données est également inscrit dans le texte. Actuellement cet avis est déjà sollicité dans la pratique lorsqu'un accès est attribué nominativement à un membre de la Police.

Le nouveau paragraphe (4) est introduit dans un but de cohérence. En effet il serait incohérent de pouvoir attribuer des accès individuels au personnel civil en vertu du paragraphe (3), mais de ne pas pouvoir attribuer ces mêmes accès aux agents de police judiciaire. Il convient également de préciser que certains policiers du Service de police judiciaire n'ont pas encore la qualité d'officier de police judiciaire.

Les paragraphes (5) et (6) sont repris de l'ancien article 43, avec une adaptation des références aux différents paragraphes.

Le paragraphe 7 est reformulé afin de souligner que disposer d'un accès à un fichier n'est pas synonyme d'avoir le droit de le consulter sans motif valable.

Ad article 2

Ad paragraphe 1er

L'article 2 introduit un nouvel article 43-1 dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale et contient des dispositions relatives au traitement de données à caractère personnel qui sont applicables à tous les fichiers de la Police dans le cadre des missions légales dont elle est investie. Il s'agit des missions de police judiciaire et de police administrative ainsi que d'autres missions légales qui ne relèvent d'aucune de ces catégories, telles que les missions effectuées dans le cadre de la police des étrangers. Tous les traitements qui relèvent de l'administration interne de la Police, tels les traitements nécessaires en matière de ressources humaines, de support logistique ou financier relèvent du règlement (UE) 2016/679 (RGPD) comme dans toutes les autres administrations étatiques.

Le nouvel article 43-1, qui s'applique à tous les fichiers que la Police gère en tant que responsable du traitement conformément à l'article 1er de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale concrétise plusieurs principes prévus par la loi du 1er août 2018 précitée.

L'article 43-1 est applicable à tous les fichiers de la Police, sauf si une disposition légale spécifique prévoit des règles différentes, comme c'est par exemple le cas de la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle.

Le choix du terme « fichier » reflète la terminologie utilisée en matière de protection des données. La loi du 1er août 2018 définit le terme « fichier » comme « *tout ensemble structuré de données à*

caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ». L'article 1er, paragraphe 3 de la même loi précise notamment qu'elle s'applique aux traitements de données à caractère personnel contenues ou appelées à figurer dans un fichier, automatisés ou non-automatisés.

Ad paragraphe 2

Dans le paragraphe 2 du nouvel article 43-1 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, les restrictions générales prévues par l'article 9 de la loi du 1er août 2018 sont spécifiées par rapport aux missions de la Police. En effet, il est inévitable que de telles données figurent dans des dossiers judiciaires et se retrouvent de ce fait dans les fichiers de la Police. Par exemple, dans le cas d'une attaque d'une personne pour des motifs xénophobes ou homophobes, l'origine raciale ou de l'orientation sexuelle de la victime relève du mobile de l'infraction et doit ainsi être mentionnée dans les procès-verbaux conformément au Code de procédure pénale. Il en est de même si la Police est à la recherche d'une personne dont le descriptif est susceptible de contenir des éléments qui pourraient divulguer des informations sur ses origines ethniques et que la Police est autorisée à traiter. Toutefois, les catégories particulières de données visées à l'article 9 prémentionné doivent toujours être pertinentes et essentielles aux fins poursuivies et ne jamais constituer une fin en soi. Ceci vaut aussi pour les recherches qui peuvent être effectuées si des catégories de données particulières sont appliquées comme clés de recherches.

Le paragraphe 2 prévoit aussi les garanties appropriées pour les droits et libertés de la personne concernée requises par la loi du 1er août 2018 et précise que les données relevant de catégories particulières ne peuvent pas être reprises de manière isolée dans les fichiers de la Police mais doivent toujours avoir un rapport avec d'autres données relatives à la personne concernée. En outre, la Police doit être en mesure d'exploiter ce type de données à des fins statistiques, auquel cas les données en question sont anonymisées.

Ad paragraphe 3

Le paragraphe 3 encadre les modalités des droits d'accès des membres de la Police aux fichiers de la Police, qui doivent être conformes à l'article 3 de la loi du 1er août 2018.

Il revient à la Police, dans sa qualité de responsable du traitement, de définir les droits d'accès ainsi que les droits par rapport à d'autres traitements ou d'autre manipulations de données, telles que la modification ou la suppression de données dans les fichiers de la Police. Le paragraphe 3 du nouvel article 43-1 ne change pas ce paradigme introduit par la loi du 1er août 2018, mais il détermine certains critères que la Police doit respecter lorsqu'elle définit ces droits. Ces critères, dont plusieurs sont inspirés de l'article 44 de la loi belge sur la fonction de police, contribuent à ce que les droits d'accès et traitement de données respectent les principes du *need to know* et *need to do*. Suivant le principe de proportionnalité, les profils et modalités d'accès sont attribués en fonction de l'emploi effectif qu'occupe le membre de la Police.

Les profils et les modalités d'accès et de traitement doivent tenir compte :

1° du détail des informations concernées auquel le membre de la Police a besoin d'accéder en raison de ses tâches. La Police met en œuvre des règles plus strictes pour l'accès à ses rapports et procès-verbaux, voire pour d'autres pièces et éléments, telles que les empreintes digitales, qui nécessiteront des droits plus étendus ;

2° du type du traitement des données : un membre de la Police qui a un accès à certaines informations n'a pas d'office les droits de *modification* ou de *suppression* de ces informations ;

3° de l'appartenance à un service déterminé ou d'une unité au sein de la Police et de la fonction du membre de la Police, ce qui empêche, par exemple, que des membres de la Police ayant des fonctions d'administration interne n'aient accès à des fichiers opérationnels de la Police, sauf si l'accès des membres des services de support dans le cadre de la gestion administrative de ces fichiers soit nécessaire ;

4° si le motif d'accès ne découle pas incontestablement de l'affectation de l'agent au sein d'un service ou d'une unité de la Police, un motif d'accès qui indique la raison de la consultation doit être fourni ;

5° de l'état de validation des données traitées. Lorsque certaines informations nécessitent encore la validation par d'autres membres de la Police, l'accès de l'agent doit être plus restreint jusqu'à ce qu'une telle validation ait eu lieu.

6° des règles spécifiques pour les données relatives à des mineurs qui prévoient que les rapports, procès-verbaux et autres pièces établis par la Police par rapport à un mineur ne peuvent être accessibles que par les membres de la section « protection de la jeunesse » du Service de police judiciaire et les officiers et agents de police judiciaire qui sont effectivement chargés d'une enquête par rapport au mineur concerné, aussi dans le cas où le mineur a le statut de victime, la Police étant chargée d'une enquête par le Parquet, soit par notice écrite soit par instruction orale, notamment dans les situations de flagrant délit, ou par ordonnance d'un juge d'instruction. Il en va de même si le service central d'assistance social est chargé d'une enquête par le Parquet ou s'il effectue des enquêtes pour le juge de la jeunesse ou le juge aux affaires familiales, et qu'il s'adresse aux commissariats de Police pour obtenir des informations complémentaires sur le mineur visé par l'enquête. En effet, l'objet de l'enquête n'est pas toujours en relation avec un fait pénal qui relève de la compétence de la section « protection de la jeunesse » du Service de police judiciaire, mais peut aussi être lié à l'environnement dans lequel le mineur évolue et qui peut être mieux évalué par les agents des commissariats au niveau local.

Le paragraphe 3, alinéa 2 adresse également la problématique de la demande de consultation d'un fichier par un autre membre de la Police que celui qui l'effectue. Dans ce cas, les données de journalisation du fichier doivent faire mention de l'identité du membre de la Police à l'origine de la demande et du motif de cette demande.

Ad paragraphe 4

Conformément à l'article 4 de la loi du 1er août 2018, la durée de conservation des données doit être définie par le responsable du traitement pour chaque fichier particulier. Toutefois, le paragraphe 4 prévoit une limitation maximale de cette durée, en précisant que pour les fichiers autres que le fichier central, la durée de conservation ne peut pas être supérieure à celles qui sont applicables au fichier central, sauf si une disposition légale spécifique prévoit une durée plus longue.

Ad paragraphe 5

Les données de journalisation collectées conformément à l'article 24 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont conservées pendant au moins cinq ans. La journalisation permet de constater des violations des droits d'accès qui sont répréhensibles sur bases des article 509-1 et suivants du Code pénal et qui se prescrivent après un délai de cinq ans.

Ad article 3

Un nouvel article 43-2 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale règle de manière spécifique le fichier central de la Police.

Ad paragraphe 1er

La vocation primaire du fichier central est de centraliser les données à caractère personnel et informations relatives aux personnes concernées traitées dans le cadre de l'exécution d'une mission légale de la Police.

Le fichier central centralise tous les documents, rapports et procès-verbaux que la Police est obligée de rédiger en application d'un texte légal ou réglementaire. En l'absence d'une centralisation, ces documents risqueraient de se retrouver éparpillés à divers endroits et dans une multitude de fichiers, conservés au niveau régional voire local, certes plus difficilement accessibles pour les membres de la Police, mais également avec des possibilités réduites des contrôles d'accès. La centralisation des informations est par ailleurs une conséquence directe du principe de l'exercice du droit d'accès par les personnes concernées. En effet, le responsable du traitement d'une grande administration peut beaucoup plus facilement donner suite à une demande d'accès si les données contenues dans les divers documents écrits de la Police sont centralisées, sans devoir consulter une multitude de banques de données, tel qu'il est le cas actuellement. Une telle centralisation des données a donc également comme avantage de réduire les délais d'attentes dans le cadre d'une demande d'accès.

Les auteurs du projet de loi ont veillé à préciser que le fichier central ne comporte pas les données relatives à des personnes qui ont commis une contravention, si une loi spéciale permet d'arrêter les poursuites pénales par le paiement d'un avertissement taxé et que la personne s'est acquittée de celui-ci dans le délai prévu par la loi. Il s'agit à titre d'exemple des avertissements taxés au sens de l'article 15 de loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies

publiques. Les raisons en sont d'une part qu'il s'agit d'une grande masse de données et que d'autre part l'information qu'un citoyen ait commis une contravention qu'il a réglée par le paiement d'un avertissement taxé est sans aucun intérêt pour l'accomplissement des missions légales de la Police. En cas de non-paiement dans les délais légaux, un procès-verbal doit cependant être rédigé, qui se retrouvera dans le fichier central.

Le fichier central est divisé dans une partie active et une partie passive. La partie active contient toutes les informations et données dont les membres de la Police doivent pouvoir disposer immédiatement dans le cadre de leurs missions légales, sous réserve des droits d'accès définis selon les critères prévus à l'article 43-1, paragraphe 3. A titre d'exemple, il peut s'agir des informations et données qui sont nécessaires pour les agents du terrain afin de garantir leur sécurité et d'évaluer une situation à laquelle ils sont confrontés et qui leur permettent de fournir aux membres du Parquet les informations dont ces derniers ont besoin afin de décider des suites à réserver aux différents cas de figure qui requièrent leur intervention. Dans le cadre d'enquêtes judiciaires, il peut s'agir, entre autres, des informations et données nécessaires pour élucider des infractions pénales, établir des liens entre différentes affaires, analyser des profils ou identifier des modes opératoires.

La partie passive sert d'archives du fichier central, dans lesquelles les informations et données sont transférées conformément aux règles relatives aux délais de conservation prévus aux paragraphes 9, 10 11, 13 et 14. L'accès à cette partie est strictement réglementé et n'est justifié que pour des finalités déterminées prévues au paragraphe 19 du présent projet de loi, dont notamment la prise de connaissance d'informations et données dans le cadre d'enquêtes en cours relatives à un crime ou délit. Ainsi dans un certain nombre de cas, il peut s'avérer nécessaire de recourir aux informations et données y contenues, alors qu'à titre d'exemple, la partie passive contiendra inévitablement des informations et données relatives à des affaires qui ne sont pas encore prescrites, ou où l'auteur est resté inconnu et que la première enquête n'a pas pu élucider l'infraction. La partie passive représente une balance nécessaire qui tient compte des droits fondamentaux et des intérêts légitimes des personnes concernées, d'une part entre le droit à une durée de conservation limitée et d'autre part la protection et les droits de la victime ainsi que l'intérêt public, une mesure nécessaire et proportionnée dans une société démocratique, eu égard à la finalité du traitement concerné.

Ad paragraphe 2

Le paragraphe 2 du nouvel article 43-2 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale définit les finalités du traitement de données à caractère personnel dans le fichier central.

La finalité primaire est la vérification des antécédents d'une personne dans le cadre d'une mission légale de la Police. La prise de connaissance de ces antécédents peut être d'intérêt soit dans le cadre d'une enquête relative à une infraction, ordonnée par le parquet ou un juge d'instruction, soit dans le cadre de la procédure du flagrant délit, alors que le fichier central signale les mesures à prendre suite à un signalement d'une personne sur base d'une décision d'une autorité judiciaire (p.ex. mandat d'amener) ou d'une autorité de police administrative (p.ex. retrait administratif d'un permis de conduire). Le fichier central est donc principalement un outil de travail journalier pour la Police et permet aussi, dans un souci d'efficacité policière, aux membres de la Police qui sont actifs sur le terrain d'avoir rapidement accès aux informations pertinentes sur une personne concernée. Ces informations sont indispensables pour leur autoprotection, ainsi que pour mieux pouvoir évaluer la situation qui les a confrontés à une personne concernée ou qui a justifié son interpellation, et de pouvoir adapter et orienter les démarches à suivre ou actions à entreprendre.

Le paragraphe 2 prévoit sous le point 2° que les informations et données à caractère personnel traitées dans le fichier central servent également d'appui aux enquêtes judiciaires par le biais d'analyses criminelles opérationnelles à la demande d'une autorité judiciaire, ce qui permet de recouper des données dans deux ou plusieurs enquêtes judiciaires en cours.

L'utilisation des données à des fins d'analyses criminelles stratégiques sous le point 3° vise l'analyse des phénomènes criminels à des fins de prévention et de recherche des infractions. Elles peuvent s'avérer utiles pour procéder à une analyse de l'évolution de la criminalité. Le résultat de cette analyse conduit à la définition d'une politique criminelle qui est alors mise en œuvre par la Police, et dont le résultat peut de nouveau être vérifié par une nouvelle analyse criminelle stratégique.

Le point 4° prévoit explicitement que les informations et données peuvent être utilisées à des fins de recherches statistiques. Même si cette finalité est déjà couverte par la loi du 1er août 2018, les auteurs ont opté d'inclure cette finalité pour des raisons d'exhaustivité.

Le point 5° mentionne que les données à caractère personnel des agents en charge d'un dossier peuvent être traitées. Ces informations sont nécessaires dans le contexte de l'attribution des droits d'accès.

Ad paragraphes 3 et 4

Les paragraphes 3 et 4 du nouvel article 43-2 précisent les catégories de personnes concernées traitées dans le fichier central aux fins de police administrative et de toute autre mission dont la Police est investie par la loi, respectivement aux fins de police judiciaire. Parmi ces catégories figurent celles visées par l'article 5 de la loi du 1er août 2018 qui dispose que le responsable du traitement établit, dans la mesure du possible, une distinction claire entre différentes catégories de personnes concernées, ainsi que plusieurs catégories complémentaires qui ont une utilité opérationnelle, telles que les personnes évadées, recherchées ou signalées, etc.

Le paragraphe 4 contient sous le point 10° une catégorie spécifique de personnes concernées, à savoir « *les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale, ainsi que les contacts ou associés qui sont suspectés d'avoir l'intention de participer à ces infractions ou d'en avoir connaissance, ainsi que les personnes qui peuvent fournir des informations sur ces infractions pénales* ». Les données qui relèvent de cette catégorie de personnes sont qualifiées dans le langage policier comme des données « douces » qui ne peuvent pas encore être rattachées à une infraction pénale suffisamment qualifiée afin que l'article 12 du Code de procédure pénale devienne applicable, mais qui sont néanmoins pertinentes pour les missions de prévention, de recherche et de constatation d'infractions pénales par la Police. Les informations fournies par des informateurs peuvent notamment être comprises dans cette catégorie. Ces données ne peuvent être répertoriées dans le fichier central que sous des conditions cumulatives strictes prévues à l'alinéa 2 du présent paragraphe 4. Une de ces conditions est que la fiabilité de la source et de l'information doit être évaluée suivant un code d'évaluation préalablement défini qui tient compte de la pertinence de la source et de l'information fournie dans le contexte de l'évolution de la criminalité et des phénomènes criminels pertinents.

Ad paragraphe 5

Le paragraphe 5 dispose quelles catégories de personnes prévues au paragraphe 4, donc traitées aux fins de police judiciaire, ne sont pas accessibles en fonction du motif de consultation saisi.

Ainsi les données à caractère personnel relatives aux catégories de personnes prévues sous les points 8°, 9° et 10° du paragraphe 4, qui font référence aux victimes, témoins et données douces, ne peuvent pas être consultées pour un motif autre qu'un motif de police judiciaire. Les données relatives à ces trois catégories de personnes ne sont donc pas affichées lorsque la Police effectue un contrôle dans le cadre d'une de ses missions non-judiciaires, par exemple lors d'un contrôle préventif en matière du Code de la route. Une exception concerne les missions en matière de la police des étrangers effectuées pour le compte de la Direction de l'immigration du Ministère des Affaires étrangères et européennes et qui ne relèvent ni des missions de police judiciaire ni des missions de police administrative, mais qui peuvent être considérées comme des missions administratives desquelles la Police est chargée en vertu d'une loi spéciale. En effet, le fait d'avoir été victime ou témoin dans une affaire pénale pourrait avoir un intérêt en matière de police des étrangers, p.ex. afin d'établir une résidence de fait, des relations avec d'autres personnes, une présence sur le territoire etc.

Des dispositions spécifiques règlent l'accès aux données à caractère personnel enregistrées sous la catégorie de personnes « données douces ». Si un membre de la Police effectue une consultation sur base d'un motif de police judiciaire et que la personne concernée fait l'objet d'une inscription au fichier central sous cette catégorie, les données ne sont pas affichées à l'agent consultant, mais les agents en charge de l'information seront avertis d'une telle consultation et peuvent prendre contact avec l'agent qui a effectué la consultation. Les officiers et agents de police judiciaire du Service de police judiciaire ont en principe accès direct aux données douces. Par dérogation, les agents à l'origine de l'information peuvent décider de limiter l'accès à une ou plusieurs sections du Service de police judiciaire. Ceci peut être utile pour limiter l'accès à des informations particulièrement sensibles dans certains domaines où il n'est pas indispensable de disposer directement de l'information pour des besoins opérationnels. Ainsi une donnée douce en matière de pédopornographie ne doit pas être directement accessible à un enquêteur en charge d'une affaire de stupéfiants, mais une donnée douce relative au financement du terrorisme peut avoir une utilité directe pour une enquête en matière de stupéfiants, alors qu'il est

possible que le financement ait eu lieu par le biais du trafic de stupéfiants. Dans l'hypothèse d'une perquisition en matière de flagrant délit, il est en effet primordial de disposer de l'information en temps réel, ce qui permet d'en tenir compte lors de l'exécution de la perquisition.

Ad paragraphe 6

Le paragraphe 6 permet expressément au responsable du traitement d'accorder un accès direct au fichier central aux officiers de police judiciaire de l'Administration des douanes et accises (ADA) ainsi que de l'Inspection générale de la Police (IGP).

Quant à l'ADA, l'accès au fichier central est strictement limité aux fonctionnaires, ayant la qualité d'officier de police judiciaire conformément à l'article 15 du Code de procédure pénale et à l'article 15 de la loi modifiée du 27 juillet 1993 portant organisation de l'administration des douanes et accises, pour lesquels un tel accès se justifie en raison de la nature de leurs fonctions au sein de l'ADA. Sont visés les officiers de police judiciaire affectés aux services de l'ADA qui exercent des fonctions de nature policière, à savoir l'Inspection antidrogues et produits sensibles à laquelle appartiennent la Brigade recherches et investigations et la Brigade recherches et cynotechnique, et l'Inspection opérations sécuritaires. En effet, les fonctionnaires affectés à ces services sont notamment impliqués dans la recherche et la constatation d'infractions pénales, le cas échéant, en flagrant délit pour lesquelles une consultation directe du fichier central s'avère utile, voire indispensable pour ne pas compromettre le bon déroulement de l'enquête. Au-delà de ces cas de figure, l'accès se justifie en raison des liens qui existent entre les enquêtes menées par l'ADA et celles menées par la Police grand-ducale dans les mêmes matières, comme par exemple la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie. Les accès ne pourront être accordés qu'aux officiers de police judiciaire nommément désignés par le directeur de l'Administration des douanes et accises, qui veillera à les désigner en fonction des besoins légaux justifiés.

Un accès direct peut également être accordé par le responsable du traitement aux membres de la l'IGP qui, en tant qu'instance d'enquête dans les domaines pénal, disciplinaire et administratif, doit pouvoir accéder directement au fichier central. Ledit accès est toutefois limité aux seuls membres de l'IGP qui ont la qualité d'officiers de police judiciaire.

Ad paragraphe 7

Le fichier central est conçu d'une telle façon que lors d'une recherche par le biais des données à caractère personnel, une page de couverture s'affichera dans un premier temps, qui permet aux agents du terrain de prendre connaissance dans l'immédiat des « informations principales » énumérées au paragraphe 7 (nom, adresse, etc.) ainsi qu'un résumé sommaire des faits dans lesquels la personne est impliquée. Ce résumé peut également comprendre les mesures que les autorités compétentes ont ordonné de prendre à l'égard de la personne concernée, et permet par exemple, à un membre de la Police de voir lors d'un contrôle si une personne est recherchée ou fait l'objet d'un mandat d'amener.

Afin d'illustrer l'importance de l'affichage de ces informations principales, on peut citer l'exemple d'une patrouille, qui pendant la nuit remarque une voiture qui circule dans un quartier où plusieurs cambriolages ont récemment été commis. Alors qu'aucune infraction n'a encore été commise, un contrôle de la Police aurait forcément un caractère préventif dans le cadre de sa mission de police administrative. Dans ce cas, la patrouille peut consulter les informations principales des personnes en question, p.ex. sur la base de la plaque d'immatriculation de la voiture et peut voir si elles ont déjà été verbalisées, voire condamnées pour des faits de cambriolage. Munis de cette information, les agents concernés peuvent procéder à une observation au sens du Code de procédure pénale au lieu de devoir procéder à un contrôle direct des personnes concernées, ce qui aurait comme conséquence que les suspects seraient avertis de la présence policière. Par contre, le détail des procès-verbaux et rapports dont la personne a fait l'objet ne sont accessibles qu'en fonction des droits d'accès et des motifs de la consultation, lesquels sont plus stricts que ceux pour un accès aux informations principales.

Le paragraphe 7 énumère les catégories d'informations et données à caractère personnel qui peuvent être traitées par rapport aux personnes physiques et morales visées aux paragraphes (3) et (4). Ces données peuvent être consultées par le personnel habilité à cette fin. Une recherche peut se faire sur base du nom complet ou partiel de la personne ou sur base d'une des autres catégories d'informations énumérées au présent paragraphe. Ces énumérations visent donc les données à caractère personnel qui peuvent être traitées si elles sont disponibles. Il s'agit de données qui figurent dans des documents

élaborés par la Police en application d'une disposition légale. Les données ont donc déjà fait l'objet d'un traitement dans la mesure où elles ont par exemple été collectées dans le cadre d'une procédure pénale. Le traitement en soi a déjà eu lieu en amont de l'enregistrement dans le fichier central.

Ad paragraphe 8

Le paragraphe 8 détermine le moment auquel les données peuvent être répertoriées dans le fichier central. Avec l'enregistrement d'un procès-verbal ou rapport dans le fichier central, les informations et données deviennent accessibles à l'ensemble des officiers et agents de police judiciaire de la Police qui disposent d'un droit d'accès en vertu de l'article 43-1, paragraphe 3. Or, ces informations et données peuvent être couvertes par le secret de l'enquête voire le secret de l'instruction. Il importe donc de trouver un équilibre entre le besoin évident de l'échange d'informations et du secret de l'enquête. Bien qu'une multitude de cas de figures puisse se produire, deux exemples sont fournis pour illustrer les intérêts à respecter.

L'information qu'un véhicule a fait l'objet d'un vol ou a été utilisé dans le cadre d'un hold-up doit être accessible immédiatement aux agents qui retrouvent ce véhicule peu de temps après qu'il a été abandonné, même si l'enquête ou l'instruction ne soient pas encore clôturées.

Par contre, le rapport dans lequel un officier de police judiciaire sollicite une écoute téléphonique ou une perquisition dans le cadre d'une enquête de laquelle il est en charge, ne peut pas se retrouver immédiatement dans le fichier central.

La loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière permet l'échange de données issues d'enquêtes judiciaires si l'enquête est terminée ou après autorisation du magistrat en charge si l'enquête est toujours en cours. Il en découle que les données à caractère personnel et les informations prévues aux paragraphes (3) et (4) sont transmises au fichier central si l'enquête est terminée, ou si l'autorité judiciaire compétente a autorisé la transmission.

Dans le cadre d'une mission de police administrative ou d'une mission administrative, les données et informations seront transmises au fichier central dès que le rapport qui les contient a été expédié aux autorités compétentes. Il peut s'agir des rapports prévus à la section 1ère du chapitre 2 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ou bien des rapports administratifs prévus dans des lois spéciales comme à titre d'exemple, celles relatives à la police des étrangers ou au Code de la route.

Ad paragraphes 9, 10 et 11

Les paragraphes 9, 10 et 11 traitent des principes relatifs aux durées de conservation applicables aux informations, données à caractère personnel et aux documents contenus dans la partie active du fichier central dans le cadre des missions de police judiciaire. Ces principes s'appliquent uniquement aux informations et données issues de rapports et procès-verbaux adressés aux autorités judiciaires pour crimes et délits, alors que celles en relation avec des contraventions sont soumises à des règles spécifiques prévues au paragraphe 17.

Les données « judiciaires » pour des fins de la vérification des antécédents dans la BNG en Belgique respectivement dans le fichier du traitement des antécédents judiciaires (TAJ) en France sont soumises à des délais de conservation qui sont nettement supérieurs aux délais de prescription, afin de prendre en compte des évènements d'interruption ou de suspension suite aux actes des autorités judiciaires qui sont entrepris dans un dossier déterminé. Ainsi, en Belgique le délai de conservation pour crimes est de trente ans, tandis que le délai de prescription est de quinze ans pour les crimes non-correctionalisables et de dix ans pour les crimes correctionalisables. La durée de conservation précitée est suivie d'une période d'archivage de trente ans. En France, le délai de conservation dans le TAJ est en principe de vingt ans. Cette durée peut être réduite à cinq ans (p.ex. pour certains délits prévus par le code de la route) ou être portée à quarante ans pour certaines infractions graves (p.ex. empoisonnement, enlèvement, prise d'otage, meurtre etc.), tandis que les délais de prescription en France sont, en principe, d'un an pour les contraventions, de six ans pour les délits, et de vingt ans pour les crimes, respectivement de trente ans pour certains crimes graves.

Un tel mécanisme suppose que la qualification exacte de l'infraction soit connue à l'avance, bien qu'en réalité la qualification ne soit connue avec précision qu'au moment d'une décision définitive en justice.

Au Luxembourg, en raison de la taille du pays, il est possible d'envisager une solution nettement plus adaptée pour prendre en compte la gravité réelle d'une infraction plutôt que de se baser sur l'infraction libellée dans le rapport de la Police, sans savoir si cette qualification sera retenue par les autorités judiciaires compétentes et sans tenir compte des circonstances atténuantes ou aggravantes qui peuvent entourer une infraction.

La police judiciaire est exercée sous la direction du procureur d'Etat et la Police exécute les délégations des juridictions d'instruction et défère à leurs réquisitions lorsqu'une information est ouverte. Comme la Police agit donc sur instruction des autorités judiciaires, le traitement des informations et données dépend largement des besoins des autorités judiciaires et ne peut pas être considéré séparément du dossier relatif à la poursuite pénale.

Concernant les délais de conservation des données à caractère personnel, il est primordial de souligner qu'il y a une différence entre les informations et données qui se trouvent dans un rapport ou procès-verbal dans le fichier central, et celles sur base desquelles une recherche doit pourvoir être effectuée ou affichera un résultat. Si dans un rapport ou procès-verbal deux personnes sont verbalisées puisqu'elles sont suspectées d'avoir commis une infraction, les informations et données relatives à ces deux personnes se trouvent dans le même document. Si à l'issue de la poursuite pénale, une de ces personnes bénéficie d'un acquittement ou est condamnée à une peine plus légère que l'autre personne impliquée, la durée de conservation des informations et données relatives à cette personne est différente de celle applicable à la personne qui a subi des condamnations plus lourdes. Dans ces cas, une consultation du fichier central sur la personne acquittée ou réhabilitée ne fournit plus de réponse, elle est donc « inconnue au fichier » sous le statut de suspect ou condamné. Cependant, il est évident que dans les détails des procès-verbaux ou rapports elle continue à figurer et que ces documents sont accessibles par le biais d'une requête qui concerne une des autres personnes pour lesquelles les limites de conservation dans le fichier central ne sont pas encore atteintes.

Ad paragraphe 9

En présence d'une condamnation coulée en force de chose jugée, la durée de conservation des informations et données dans le fichier central de la Police est liée à la durée pendant laquelle la condamnation figure au casier de la personne concernée. La réhabilitation de la personne condamnée entraîne donc automatiquement le transfert des informations et données dans la partie passive du fichier central. Si la réhabilitation ne concerne pas toutes les personnes condamnées, les informations et données sont maintenues en partie active jusqu'à la réhabilitation de toutes les personnes condamnées dans une affaire déterminée. La raison en est que les documents relatifs à une poursuite pénale ne peuvent pas être disjoints ou modifiés à posteriori, alors qu'en règle générale ils sont rattachés à une affaire déterminée et non individuellement à toutes les personnes physiques impliquées dans l'affaire visée. Toutefois, afin de respecter le principe général que les informations et données sont à transférer dans la partie passive dès qu'une personne concernée est réhabilitée, la personne déjà réhabilitée dans une affaire déterminée ne pourra plus être recherchée par le biais de ses données à caractère personnel à partir de la suppression de la condamnation de son casier judiciaire pendant le maintien des documents en partie active. Il y a donc une suppression du lien entre la personne réhabilitée et l'affaire visée tant que les documents relatifs à la poursuite pénale sont maintenus dans la partie active du fichier central.

Les principes des délais de conservation retenus dans le paragraphe 9 rejoignent le modèle français dans le sens que l'article 230-8 du Code de procédure pénale français prévoit qu'une demande d'effacement ou de rectification des données à caractère personnel d'une personne concernée ne peut être formulée que lorsque ne figure plus aucune mention de nature pénale dans le bulletin n°2 de son casier judiciaire, qui comporte la plupart des condamnations et décisions de justice sauf quelques exceptions.

Par rapport à la durée de conservation fixe de dix ans dans l'ancien fichier central, ce principe a comme avantage qu'une personne condamnée ne peut plus devenir « inconnue au fichier » alors qu'elle est toujours en train de purger sa peine. En effet, pour les besoins de la sécurité intérieure, la Police doit disposer des informations relatives à une personne qui a une inscription dans son casier.

Dès qu'il y a condamnation d'un prévenu, il n'est plus nécessaire de pouvoir rechercher les victimes et témoins dans la partie active du fichier central. Une exception est cependant nécessaire dans l'hypothèse d'une disjonction des poursuites, alors que la recherche d'un ou de plusieurs auteurs présumés de l'infraction continue.

Ad paragraphe 10

Le paragraphe 10 fixe le principe des délais de conservation en présence d'une décision d'acquittement coulée en force de chose jugée. Tout d'abord, ce principe prévoit que les informations et données de la personne concernée sont transférées dans la partie passive du fichier central si elle bénéficie d'un acquittement à l'issu d'une poursuite pénale. Il s'agit d'un automatisme dès que les décisions y relatives parviennent à la Police par retour d'informations automatisé du traitement dit chaîne pénale des autorités judiciaires (JUCHA). Le procureur d'Etat a toutefois la possibilité de décider de maintenir les informations et données dans le JUCHA, et par extension dans le fichier central de la Police, s'il le juge nécessaire pour des raisons liées à la poursuite pénale. Ce système suit ainsi le principe prévu dans l'article 230-8 du Code de procédure pénal français, lequel dispose que les données à caractère personnel des personnes acquittées sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elles font l'objet d'une mention.

Le principe du transfert immédiat des informations et données dans la partie passive n'est pas applicable en tant que tel si plusieurs personnes sont impliquées dans une affaire déterminée et qu'elles n'ont pas toutes bénéficié d'un acquittement, ou si après l'acquittement d'une personne concernée la recherche de l'auteur de l'infraction continue. Les documents, qui contiennent des informations et données relatives à toutes les personnes impliquées, restent rattachés à la poursuite pénale en cours et doivent être maintenus en partie active, alors qu'ils ne peuvent pas être disjoints ou modifiés à la suite de l'acquittement d'une des personnes concernées.

Toutefois, dans ces deux cas de figure, il y a suppression du lien entre la personne acquittée et les documents relatifs à la poursuite pénale, de sorte que lors d'une recherche sur la personne acquittée elle sera « inconnue au fichier » sous le statut de suspect, tant que les documents relatifs à la poursuite pénale doivent être maintenus en partie active. Ces documents peuvent rester accessibles sur la base d'une recherche par rapport aux données des autres personnes impliquées et non-acquittées dans l'affaire. Ainsi, dans le cas d'une infraction reprochée à un groupe de suspects dont un bénéficie d'un acquittement, une recherche à partir du nom de l'acquitté ne donnera plus aucun résultat, mais une recherche à partir du nom d'un des auteurs condamnés permettra d'accéder aux documents dans lesquels le nom de l'acquitté continue à figurer. Il en est de même lorsque la recherche pour l'auteur de l'infraction continue et que les documents existants relatifs à la poursuite pénale sont consultés dans le cadre de cette enquête. Il échet toutefois de noter qu'il est également possible qu'une personne suspecte ait initialement été entendue comme témoin dans les phases initiales de l'enquête. Dans ce cas, elle conserve ou retrouve son statut de témoin après son acquittement, mais ne figurera plus sous le statut de suspect dans le dossier. En effet, il est impossible de réécrire les procès-verbaux et rapports en question. Dans ce contexte, il est également renvoyé aux explications sous « ad paragraphes 9, 10 et 11 ».

Si l'enquête est reprise suite à un acquittement ou dans le cas d'une disjonction des poursuites qui aboutirait à l'acquittement du prévenu renvoyé devant le juge et où l'enquête est toujours en cours pour rechercher les autres auteurs de l'infraction, il est nécessaire de garder les données relatives aux victimes et témoins dans la partie active. En l'absence de reprise de l'enquête ou d'autres personnes suspectes impliquées dans l'affaire, les informations et données relatives aux témoins et victimes sont transférées dans la partie passive du fichier central, et subissent ainsi le même sort que les informations et données de la personne acquittée dans la même affaire. Quant à l'opportunité de maintenir des informations et données dans la partie passive, l'accès à laquelle est très restreint et limité à des finalités déterminées, il est renvoyé aux explications sous les paragraphes 1 et 19 de l'article 43-2.

Dernièrement, il convient de noter qu'une personne peut être condamnée pour un fait sous une des qualifications pour lesquelles elle avait été renvoyée devant le juge, mais bénéficier d'un acquittement pour une autre. Elle serait donc tenue coupable pour les faits, mais acquittée pour une qualification retenue à tort. Dans un tel cas, il est clair que ce sont les principes des délais de conservation relatifs aux décisions de condamnations qui sont applicables.

Ad paragraphe 11

En l'absence d'une décision coulée en force de chose jugée, les auteurs du projet de loi ont prévu de s'aligner sur le concept d'archivage appliqué par les autorités judiciaires au traitement, dit chaîne-pénale (JUCHA) du ministère public. Le paragraphe 11 vise les décisions de non-lieu, de classements sans suites, ainsi que les affaires dans lesquelles l'auteur est resté inconnu ou les affaires prescrites qui sont mises « ad acta » et pour lesquelles aucune décision n'est intervenue.

Dans ces cas, les documents, informations et données à caractère personnel sont archivés, respectivement transférés dans la partie passive du JUCHA, trois ans après le dernier acte d'instruction ou de poursuite entrepris dans une affaire déterminée. Les autorités judiciaires informeront la Police d'un tel archivage par un retour d'informations automatisé avec le fichier central, ce qui sera alors également le moment où les documents, informations et données repris au fichier central dans le cadre du dossier en question sont transférés dans la partie passive du fichier central.

La solution retenue dans le présent projet de loi a le mérite qu'il y a un alignement entre le concept d'archivage, respectivement transfert dans la partie passive, auprès des autorités judiciaires et celui de la Police. Dans les cas qui n'ont pas conduit à des poursuites, où aucune décision n'est intervenue ou qui ont été évacués par une décision de non-lieu, un « archivage » aura lieu beaucoup plus tôt tel que c'était le cas dans l'ancien fichier avec son délai fixe de dix ans de conservation, ou tel qu'est le cas en Belgique ou en France. En France, les données à caractère personnel sont en principe conservées pendant vingt ans en cas de décisions de non-lieu ou de classement sans suites, sauf si le procureur de la République ordonne leur effacement, alors qu'au Luxembourg elles seront transférées dans la partie passive dès qu'elles sont archivées au niveau du JUCHA.

Afin de réduire le nombre de dossiers où l'infraction n'est pas encore prescrite, mais qui font l'objet d'un archivage précoce en raison de l'absence d'acte de procédure pendant trois ans, et pour lesquels l'enquête pourrait être reprise, il est envisagé de porter ce délai d'archivage dans le JUCHA à cinq ans dans le futur. Toutefois, comme les délais de conservation prévus par le présent paragraphe sont relativement courts par rapport aux délais de prescription de l'action publique, il est inévitable que des infractions qui ne sont pas encore prescrites puissent se retrouver transférées dans la partie passive du JUCHA et par conséquence du fichier central. Afin de remédier à une telle situation, le paragraphe 16 de l'article 43-2 prévoit une possibilité de retransfert dans la partie active, notamment en cas de reprise des enquêtes.

Les décisions de classements sans suites et de non-lieu ont en commun qu'il ne s'agit pas de décisions définitives et qu'une condamnation reste possible jusqu'à l'atteinte de la date de prescription de l'action publique. Elles se distinguent principalement sur les modalités de reprise des charges qui sont soumises à un certain formalisme dans l'hypothèse d'une décision de non-lieu.

A côté de l'argument relatif à la possibilité de reprendre les poursuites jusqu'à la prescription de l'action publique, l'importance de pouvoir accéder à des informations et données relatives à des affaires caractérisées par l'absence de décisions coulées en force de chose jugée, telles que des décisions de non-lieu ou de classements sans suites, réside dans la prise de connaissance des antécédents d'une personne. Sur ce point, il est renvoyé aux explications fournies sous le paragraphe 2 du présent article, relatif aux finalités du fichier central.

A titre d'exemple, en matière de violences domestiques ou de stupéfiants, il est possible que pour un premier fait l'auteur bénéficie d'un classement sans suites, mais qu'il existe une forte probabilité de récidive, de sorte qu'un archivage précoce aurait comme effet que ni au niveau de la Police, ni au niveau du ministère public, une information relative au premier fait, pourtant non prescrit, ne soit encore disponible dans la partie active. En outre, lors d'une première affaire, il se peut que le ministère public décide de ne pas poursuivre et de classer une affaire sans suites comme il s'agit d'un premier fait et que les blessures de la victime n'étaient pas très graves ou la quantité de stupéfiants en possession de la personne n'était pas très élevée. Si quelques semaines plus tard, la police doit intervenir à nouveau et si on avait supprimé ou transféré les décisions de classement sans suites ou de non-lieu, l'auteur serait « inconnu au fichier ». Toutefois, en dehors des heures de bureau, le substitut de permanence qui est informé des faits n'a pas accès au JUCHA, et si l'auteur est inconnu au fichier, le substitut pourrait décider de se limiter à rédiger procès-verbal au lieu d'ordonner d'autres mesures plus appropriées.

Dans ce contexte, il convient encore de noter que le rapport au gouvernement pour l'année 2019 du Comité de coopération entre les professionnels dans le domaine de la lutte contre la violence souligne l'importance de pouvoir réévaluer une situation, ainsi que la prise en compte des antécédents spécifiques des auteurs (p.ex. tendance à un comportement violent, abus d'alcool ou de stupéfiants récurrent) qui, notamment pour des raisons d'opportunité des poursuites, n'ont pas été sanctionnés par une condamnation ou qui ne sont pas sanctionnables (p.ex. incidents psychiatriques). Le Comité estime même que la durée de conservation de dix ans actuellement pratiquée au niveau du fichier central « correspond à un délai très court par rapport à sa finalité, [et que] cette application vétuste ne permet cependant pas d'effectuer des recherches sur des types d'infraction ou modes opératoires. »

Ad paragraphe 12

Un retour d'informations automatisé des suites réservées aux procès-verbaux et rapports de la Police par les autorités judiciaires garantit que toutes les décisions de justice puissent être mentionnées dans les affaires visées au niveau du nouveau fichier central. Un tel retour automatisé, qui faisait défaut dans l'ancien fichier central, permettra de garantir que les données à caractère personnel soient adéquates, exactes et tenues à jour, tel que prévu par l'article 3, paragraphe 1er de loi du 1er août 2018 précitée.

En même temps, une telle mention dans le dossier permet d'adresser une des grandes critiques qui était que les fichiers de la police reflètent la perception policière d'une situation, sans tenir compte des suites judiciaires. Il s'y ajoute que la Police est obligée d'enregistrer les plaintes des personnes qui dénoncent une infraction, même si les agents ont des doutes sur la véracité des faits. En raison des délais entre la commission d'un fait et une décision coulée en force de chose jugée, il est indispensable de pouvoir tenir compte de ces informations qui se trouvent dans les fichiers de Police avant qu'une juridiction n'ait pu trancher. Le nouveau paragraphe 12 garantit que dès qu'une décision est rendue, et alors que les procès-verbaux et rapports ne peuvent pas être modifiés pour en tenir compte, l'information relative aux suites judiciaires permet de mieux apprécier la pertinence de la perception policière initiale des faits.

Ad paragraphe 13

Le Procureur d'Etat peut cependant décider du transfert de documents, informations et données dans la partie passive, ou ordonner la suppression du lien entre une personne concernée et une affaire déterminée. Cette décision relève davantage d'une décision de poursuite pénale que d'une décision en matière de protection des données, raison pour laquelle elle appartient à une autorité judiciaire au lieu du responsable du traitement, qui continue de recevoir les demandes d'accès, d'effacement et de rectification qui relèvent de la protection des données.

Une telle décision du Procureur d'Etat pourrait par exemple se justifier dans des cas où une personne a été verbalisée à tort par la Police ou où une décision de non-lieu a été motivée par l'absence d'un fait pénal, auquel cas une reprise sur charges nouvelles est vraisemblablement exclue, alors qu'il n'y a pas de faits. La Police n'est pas compétente de prendre ces décisions elle-même en tant que responsable du traitement, si aucune disposition en matière de protection des données n'est affectée et alors qu'elle ne peut pas déroger aux délais de conservation prévus par la présente loi.

En France dans le cadre du TAJ, un système similaire est prévu dans l'article 230-8 du Code de procédure pénale, lequel permet au procureur de la République d'ordonner d'office ou à la demande de la personne concernée l'effacement ou la rectification de ses données à caractère personnel, respectivement l'apposition d'une mention. Comme en France, les décisions du procureur d'Etat sont susceptibles d'un recours, en l'occurrence devant le président du tribunal d'arrondissement compétent en la matière.

Ad paragraphe 14

Le paragraphe 14 prévoit un régime de conservation spécifique par rapport aux délais de conservation prévus aux paragraphes 9, 10 et 11, en raison du caractère spécifique de certains rapports rédigés par la Police dans le cadre de ses missions de police judiciaire.

Un régime de conservation spécifique est prévu pour les rapports rédigés dans le contexte d'une demande d'entraide judiciaire, afin de tenir compte du fait que dans ces cas il n'y a généralement pas de constatation d'une infraction au Luxembourg et donc pas d'enquête menée au niveau national. En conséquence, aucun retour d'informations automatisé ne peut avoir lieu, de sorte qu'il est nécessaire de prévoir un délai de conservation fixe après lequel ces rapports sont transférés dans la partie passive.

Le paragraphe 14, dans son alinéa 2, se réfère aux rapports adressés aux autorités judiciaires qui n'ont pas directement pour objet la constatation d'une infraction, mais qui sont néanmoins liés à une infraction qui a été constatée dans un procès-verbal ou rapport antérieur et déjà enregistré au fichier central. Il peut s'agir à titre d'exemple d'un rapport sur le placement d'un mineur, d'un rapport sur une fouille corporelle ou sur une fouille d'un véhicule, ou d'un rapport d'observation. Pour ces rapports, qui sont donc liés à un dossier pénal existant, ce sont les délais de ce dernier qui s'appliquent.

Si ces rapports ne concernent pas une enquête en cours ou une infraction pénale, ce sont les délais en matière de police administrative qui s'appliquent, et ils sont donc transférés dans la partie passive

au plus tard après une période de dix ans. Il peut s'agit à titre d'exemple d'une fouille corporelle ou d'une fouille d'un véhicule qui ont été négatives.

Ad paragraphe 15

Le paragraphe 15 prévoit un régime de conservation spécifique pour les documents, informations et données en matière de police administrative ou d'autres missions administratives de la Police.

Les informations, données et documents repris dans le fichier central dans le cadre d'une mission de police administrative ou d'une mission administrative dont la Police est investie par la loi sont supprimés au plus tard après une période de dix ans. Le fichier central a comme objectif de centraliser et de regrouper tous les écrits à un seul endroit, il convient donc de souligner qu'il ne s'agit pas de nouveaux traitements, mais de traitements de données qui existent déjà et qui seront à l'avenir regroupés à un endroit central qui est mieux sécurisé, et qui permet une gestion centrale des durées de conservation. Les rapports rédigés dans le cadre d'une mission de police administrative ou d'une mission administrative ne sont pas archivés mais supprimés de la partie active, sans préjudice cependant des dispositions légales en vigueur en matière d'archivage historique. En principe, l'application d'une mesure contraignante par la Police doit être documentée afin d'être en mesure de vérifier sa légalité *a posteriori*. Une mesure non documentée peut avoir un caractère douteux. Dans la majorité des cas, une documentation est formellement prévue par la loi et la Police doit dès lors être en mesure de prouver la licéité de ses actes.

La Police arrêtera, conformément à l'article 4 de la loi du 1er août 2018, des délais de conservation par type de rapport non-judiciaire, dont, compte tenu des principes de proportionnalité et de nécessité, certains seront plus courts que la durée maximale de dix ans. La Police tient un relevé dans lequel les délais spécifiques sont indiqués.

Dans la loi belge sur la fonction de police les délais de conservation pour des données de police administrative dans la BNG sont à la base plus brefs (3 ou 5 ans selon la catégorie des personnes concernées) mais elle prévoit aussi plusieurs possibilités de prolongation de ces délais, notamment une prolongation pour la durée qu'« *il y a une mesure à prendre sur la base d'une décision d'une autorité administrative ou judiciaire compétente* ». Dans un souci de simplification, les auteurs du projet de loi ont préféré prévoir un délai maximal plus important, ce qui évite de prévoir plusieurs exceptions de prolongation et en même temps permet une vérification de la légalité des actions de la Police.

Ad paragraphe 16

Le paragraphe 16 crée un automatisme de retransmission de la partie passive du fichier central, respectivement des fichiers particuliers, dans la partie active du fichier central, lorsqu'une telle retransmission a lieu au niveau du JUCHA. Une telle retransmission peut être justifiée pour des raisons limitativement énumérées à l'alinéa 1er.

Ainsi un retransfert dans la partie active peut s'avérer nécessaire si des circonstances de l'enquête révèlent qu'une infraction n'est pas encore prescrite, mais les pièces y relatives ont été automatiquement transférées dans la partie passive en raison de l'absence d'actes de procédure. Il en va de même dans le cas d'une reprise sur charges nouvelles conformément aux article 135 et suivants du Code de procédure pénale ou bien de l'annulation d'un classement sans suites par un procureur d'Etat.

Les deuxième et troisième raison concernent des infractions où une décision judiciaire n'a pas été prise par une juridiction de jugement au Luxembourg. Il peut s'agir de cas où une infraction a été commise au Luxembourg et qui pourrait conduire à des poursuites. Il peut s'agir de cas où une nouvelle affaire nationale est liée à un dossier qui a conduit à une demande d'entraide judiciaire internationale antérieure et où les éléments de cette enquête doivent être considérés dans le nouveau dossier, même si les faits étaient entretemps prescrits ou qu'une décision définitive soit intervenue au fond au niveau d'une juridiction d'un autre Etat, auquel cas le principe du *non bis in idem* pourrait s'appliquer.

La distinction fondamentale entre l'accès à la partie passive, prévu au paragraphe 19, et le retransfert dans la partie active prévu au paragraphe 13, indépendamment des conditions légales auxquelles il est soumise, est que dans le cas de l'accès à la partie passive, l'accès se limite à un nombre très restreint d'agents, alors que dans le cas du retransfert, les informations sont accessibles à tous les agents qui disposent un droit d'accès au fichier central conformément aux règles prévues à l'article 43-1, paragraphe 3.

Ad paragraphe 17

En principe, les informations et données sont supprimées au plus tard trente ans après leur transfert dans la partie passive. Il est toutefois possible que les informations et les documents y afférents ne

soient pas supprimés totalement, dans la mesure où ils peuvent se retrouver aux archives nationales sur la base de la loi du 17 août 2018 relative à l'archivage.

A l'instar des délais de conservation dans la partie active, un délai plus court de trois ans est prévu pour les données douces dans la partie passive.

Une autre dérogation concerne les informations et données qui proviennent de procès-verbaux ou rapports pour contraventions, où les auteurs ont prévu un effacement cinq ans après l'établissement du procès-verbal ou rapport, conformément aux principes de proportionnalité et de nécessité en matière de protection des données. D'une part, une conservation de ces informations et données dans la partie passive n'est pas nécessaire d'un point de vue opérationnel, et d'autre part un retour d'informations automatisé tel que prévu par les paragraphes 9, 10 et 11 n'est pas possible en raison du régime spécifique applicable à certains types de contraventions. Le délai de cinq ans permet de tenir compte des différents cas de récidives en matière de contraventions ainsi que des voies de recours qui peuvent étendre le temps de clôture d'une affaire et à partir de laquelle court le délai pendant lequel une récidive est possible. En outre, un délai de conservation de cinq ans semble proportionné, alors que la réhabilitation de droit pour toute condamnation à des peines de police est acquise après un délai de cinq ans.

Ad paragraphe 18

Le paragraphe 18 règle la relation entre les informations et données judiciaires contenues dans le fichier central et celles qui se trouvent dans d'autres fichiers particuliers. Ces dernières doivent être supprimées au moment du transfert des informations correspondantes dans la partie passive du fichier central. Si les délais de conservation du fichier central sont atteints, les informations et données ne peuvent donc en principe plus être conservées dans un fichier particulier, sauf pour les fichiers qui sont régis par une disposition légale spécifique qui prévoit une durée de conservation différente, telle que par exemple la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle.

Une exception doit néanmoins être prévue pour les informations et données contenues dans d'autres fichiers dans un format qui ne peut pas être géré par le fichier central. L'alinéa 2 dispose que ces dernières peuvent être archivées dans le fichier particulier s'il dispose d'une possibilité d'archivage. C'est par exemple le cas pour les empreintes digitales où les images dactyloscopiques sont transformées par un algorithme en un code unique qui sert aux comparaisons, lesquelles ne peuvent pas être effectuées dans le fichier central. Les durées d'archivage et les conditions d'accès sont alors les mêmes que celles prévues pour la partie passive du fichier central.

Une autre exception est nécessaire pour les traces prélevées sur des lieux où les auteurs des infractions sont restés inconnus. En effet chaque année environ 20 000 infractions sont signalées pour lesquelles les auteurs sont inconnus au moment du constat. Même après l'enquête, pour beaucoup d'entre elles les auteurs restent inconnus alors que des traces qui pourraient servir à leur identification ont été prélevées. Si toutes les mesures d'enquête ont été accomplies par la Police et les autorités judiciaires compétentes, l'inactivité consécutive dans le dossier entraîne un archivage dans le JUCHA au bout de 3 ans. Or, un grand nombre de ces infractions sont des cambriolages ou autres vols aggravés qui sont des crimes qui ne se prescrivent qu'au bout de dix ans après le dernier acte interruptif. Un archivage des traces, notamment des empreintes digitales, aurait comme effet qu'il serait impossible d'élucider un fait grave non encore prescrit, si l'auteur était arrêté pour un autre fait, alors que le premier fait ne soit pas encore prescrit et que ses empreintes permettraient de le lier au premier ou à d'autres faits. Il s'y ajoute que le délai de prescription peut s'allonger considérablement si les faits ont été commis dans le cadre d'une organisation criminelle ou d'une association de malfaiteurs.

Ad paragraphe 19

Dès le transfert dans la partie passive, l'accès aux informations et données à caractère personnel est soumis à des droits d'accès et de consultation très stricts. Le projet de loi énumère de manière exhaustive les finalités qui peuvent justifier la consultation des informations et données contenues dans la partie passive du fichier central :

1° la prise de connaissance des informations dans le cadre d'une enquête en cours relative à un crime ou à un délit ;

2° la prise de connaissance des informations dans le cadre d'une demande en révision conformément aux articles 443 et suivants du Code de procédure pénale.

La partie passive contient des informations et données qui suivant les règles définies aux paragraphes 9, 10, 11, 13 et 14 de l'article 43-2 ont été transférées de la partie active du fichier central dans la partie passive. Dans la majorité des cas les informations et données contenues dans la partie passive ne peuvent plus servir à relancer des poursuites, toutefois elles peuvent fournir des indices importants, par exemple pour établir des liens entre personnes ou entre différentes affaires, ou pour comparer des modes opératoires afin de contribuer à élucider des faits nouveaux. La partie passive peut cependant aussi contenir des infractions non encore prescrites, si l'auteur de l'infraction est resté inconnu, ou si une décision de classement sans suite ou de non-lieu a été rendue et où la poursuite peut encore être reprise. Dans la plupart de ces cas, il sera cependant procédé à un retransfert, conformément au paragraphe 16. A titre d'exemple, suite à l'élucidation d'un fait lors duquel un mode opératoire bien spécifique a été employé, un enquêteur peut s'intéresser à d'autres faits où un mode opératoire semblable a été utilisé. Il est possible que certains faits soient prescrits et d'autres pas.

Pour cette raison, il peut s'avérer utile d'autoriser l'accès à la partie passive du fichier central à un nombre d'enquêteurs très limité, actifs dans un domaine de criminalité particulièrement grave comme à titre d'exemple le terrorisme ou la criminalité organisée. En effet, en matière de terrorisme, il arrive fréquemment que des personnes radicalisées ont un passé de « petits délinquants », des faits qui en raison des délais de conservation prévus aux paragraphes 9, 10, 11, 13 et 14 pourraient se retrouver relativement vite dans la partie passive, alors que l'existence même de ces faits permettrait de mieux apprécier le danger qui pourrait résulter suite à leur radicalisation présumée. Par ailleurs, le type d'infraction commise (p.ex. vols par emploi d'explosifs) ou les contacts que ces personnes ont entretenu à l'époque pourraient également servir à mieux évaluer le danger potentiel.

Une consultation de la partie passive sur une période déterminée peut également s'avérer utile s'il s'agit par exemple d'élucider des faits graves qui se sont déroulés pendant une certaine période de temps et où les enquêtes seraient toujours en cours, comme à titre d'exemple une série d'attentats au moyen d'explosifs ou un meurtre.

La deuxième raison d'accès concerne une demande en révision conformément aux articles 443 et suivants du Code de procédure pénale.

A l'instar du règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, où l'accès à la partie archivage de INGEPOL relevait de la compétence du Procureur général d'Etat, l'accès à la partie passive du nouveau fichier central est soumis à l'accord du procureur général d'Etat ou à un des membres de son parquet désignés à cet effet. Pour la première finalité sous le point 1°, une telle consultation peut également avoir lieu sur demande du juge d'instruction en charge de l'enquête.

A côté des consultations ponctuelles, le procureur général d'État peut autoriser l'accès aux informations contenues dans la partie passive du fichier central à des officiers et agents de police judiciaire nominativement désignés du Service de police judiciaire ou aux membres de certaines subdivisions du Service de police judiciaire pendant une durée maximale de cinq ans renouvelable.

Le délégué à la protection des données de la Police a également accès aux informations et données contenues dans la partie passive si cela est requis dans le cadre de l'exercice du droit d'accès de la personne concernée en vertu de l'article 13 de la loi du 1er août 2018. Il en va de même pour l'Inspection générale de la Police dans le cadre de ses missions en vertu de l'article 12 de la loi modifiée du 18 juillet 2018 sur l'Inspection générale de la Police.

Il convient également de préciser que ces règles ne privent pas une personne concernée d'exercer son droit d'effacement au sens de l'article 15, paragraphe 2 de la loi du 1er août 2018. Dans le cas où un effacement en vertu de cette disposition est justifié, la Police peut dans les limites de l'article 15, paragraphe 3 de la même loi limiter le traitement en question, étant entendu que cette limitation peut prendre la forme d'un transfert des données en question vers la partie passive du fichier central.

Ad article 4

L'article 4 insère un nouvel article 43-3 dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, qui désigne la Police grand-ducale comme responsable du traitement des traitements de données à caractère personnel qu'elle effectue.

Jusqu'à présent, ni la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ni la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ne précisent, de manière générale,

le responsable des traitements de données opérés par la Police. Dans son avis complémentaire du 12 mai 2020 relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, qui a comme objet d'encadrer la vidéosurveillance par la Police, le Conseil d'Etat avait émis une proposition d'insérer la disposition désignant le responsable du traitement sous un article distinct dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale de façon à garantir ainsi son application à l'ensemble des traitements de données à caractère personnel effectués par la Police[2]. Les auteurs du projet de loi ont suivi cette proposition par l'insertion du nouvel article 43-3.

Le projet de loi n°7498 susmentionné avait par amendement gouvernemental d'avril 2020 proposé de remplacer la désignation du directeur général de la Police comme responsable du traitement par « la Police grand-ducale, représentée par son directeur général ». D'une part, les auteurs sont conscients que d'autres lois en matière policière font référence au « directeur général de la Police » comme responsable du traitement, et se proposent d'adapter la désignation du responsable du traitement dans ces lois dans le futur. D'autre part, compte tenu des critiques du Conseil d'Etat relatives à l'utilisation de la notion de « représentation » dans leur avis du 12 mai 2020, les auteurs ont opté de faire abstraction de cette terminologie et de désigner la Police grand-ducale tout court comme responsable du traitement.

Le mépris des obligations légales du responsable du traitement peut entraîner des sanctions de nature administrative, et sous certaines conditions, de nature pénale ou faire l'objet de dommages et intérêts en matière civile. Pour cette raison, et après consultation des experts en matière de protection des données, les auteurs estiment qu'il n'est pas opportun de désigner une personne physique individuelle comme responsable du traitement de traitements opérés par une administration étatique ou toute autre autorité publique. Ainsi il convient de désigner l'administration, en l'occurrence la Police grand-ducale, comme responsable du traitement.

Cette approche rejoint d'ailleurs l'esprit des textes européens, lesquels dans la directive (UE) 2016/680, article 3, point 8, ont défini le responsable du traitement comme « *l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou le droit d'un État membre* »; et dans le règlement (UE) 2016/679 (RGPD), article 4, point 7, comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* ».

En outre, les « Guidelines 07/2020 on the concepts of controller and processor in the GDPR » de l'EDPB ont retenu que:

> « *17.* […] *In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR.[…].*
>
> *18. Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing operations. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller.* »

Il en résulte que c'est l'administration ou l'entité publique en tant que tel qu'il convient de désigner comme responsable du traitement des traitements opérés par cette dernière.

Ad article 5

Il y a lieu de supprimer dans la loi portant réorganisation du Service de renseignement de l'Etat la disposition conférant au Service de renseignement de l'Etat l'accès à une banque de données que le présent projet de loi vise à supprimer.

---

2 Avis complémentaire du Conseil d'Etat, N° CE : 60.043, relatif au projet de loi portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, N°7498/04, session ordinaire 2019-2020.

Ad article 6

Un consensus politique a émargé de prévoir des sanctions pénales à l'égard des membres de la Police grand-ducale qui commettent un abus de leurs droits d'accès aux différents fichiers de la Police.

Le système des sanctions pénales prévues par la loi modifiée du 2 août 2002 précitée a largement été remplacé par un système de sanctions administratives par le règlement UE 2016/679 (RGPD) et la directive UE 2016/680, transposée en droit luxembourgeois par loi du 1er août 2018, suite à un consensus au niveau européen, ayant constaté l'inefficacité des sanctions pénales existantes. Ainsi les auteurs ont estimé qu'il serait incohérent de réintroduire des sanctions pénales similaires à celles qui existaient avant 2018 et qui ont été abolies.

Il s'y ajoute que dans son troisième avis complémentaire relatif au projet de loi portant création de l'Autorité nationale de sécurité, le Conseil d'Etat a émis une opposition formelle quant à l'application simultanée des dispositions de la loi du 1er août 2018 et des sanctions pénales tirées de la loi modifiée du 2 août 2002 précitée et insérées dans le projet de loi n° 6961.[3] Le Conseil d'Etat a observé qu'une telle application simultanée, associée aux divergences de formulation entre les dispositions concernées, est source d'insécurité juridique et il a demandé la suppression de l'amendement qui visait à réintroduire des sanctions pénales tirées de la loi modifiée du 2 août 2002 précitée.

En outre, les auteurs ont estimé qu'une incrimination spécifique à l'égard des membres de la Police dans la loi sur la Police soulèverait des questions quant au respect du principe constitutionnel d'égalité et de non-discrimination, en ce qu'une telle incrimination spécifique n'est pas prévue pour les membres d'autres autorités compétentes qui relèvent aussi de la loi du 1er août 2018.

Afin de satisfaire aux exigences de sanctions pénales en matière de violations des droits d'accès, et ce à l'égard de toutes les autorités étatiques et entités privées, les auteurs proposent de procéder à la modification des articles 509-1 et suivants du Code pénal, qui couvrent déjà un grand nombre de cas de violations frauduleuses des droits d'accès, mais bénéficieront d'adaptations afin d'étendre leur champ d'application, en vue des jurisprudences en la matière et les réalités opérationnelles des différentes autorités compétentes.

Alors que l'article 509-1 et suivants ne s'appliquent qu'aux systèmes informatiques, il convient tout d'abord d'étendre leur champ d'application également aux traitements de systèmes non-automatisés, où approprié.

Il convient par ailleurs de tenir compte des jurisprudences en la matière.[4] Le délit de l'article 509-1 du Code pénal réprime non seulement l'accès frauduleux à un système de traitement ou de transmission automatisé de données, mais également le maintien dans le système. L'un ou l'autre suffit à caractériser l'élément matériel du délit ; le fait d'accéder de manière autorisée à un serveur ou à un réseau n'implique pas que le maintien dans le système soit forcément régulier. La jurisprudence admet que le fait pour un employé, autorisé à accéder de manière inconditionnelle au réseau pour exécuter des tâches relevant de son activité, de se maintenir dans le réseau pour exécuter des opérations non autorisées rend le maintien frauduleux.

Les juridictions ont ainsi interprété l'article 509-1 de manière que même si *l'accès en lui-même* à un fichier n'est pas frauduleux, le fait de se *maintenir* dans une banque de données à des fins autres que les finalités licites pour lesquelles l'autorisation d'accès a été attribuée est considéré frauduleux. Les modalités d'accès ne doivent donc pas être explicitement frauduleuses, alors qu'elles ne le sont pas si un agent dispose d'un accès licite, or le fait d'utiliser cet accès à des fins privées ou pour des finalités pour lesquelles l'agent n'est pas habilité doit être clairement couvert par les dispositions du Code pénal.

Les auteurs proposent donc d'ajouter un nouvel alinéa 2 à l'article 509-1, qui vise spécifiquement les données à caractère personnel et incrimine toute personne qui effectue un traitement de données à caractère personnel pour des finalités autres que celles pour lesquelles l'autorisation d'accès a été accordée. Il est précisé que l'incrimination vise aussi le fait de porter à la connaissance d'un tiers non autorisé les données à caractère personnel ainsi obtenues.

---

3 Troisième avis complémentaire du Conseil d'Etat, N°CE : 51.569, N° dossier parl. : 6961 relatif au projet de loi porant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

4 Tribunal d'Arrondissement, 15 juin 2011, no 2025/2011 ; Cour d'appel, 27 juin 2012, no 342/12 ; Cour d'appel, 31 mars 2015, no 133/15.

Ad article 7

L'article 6 prévoit une date butoir pour la mise en conformité des fichiers particuliers de la Police avec les dispositions du présent projet de loi, ainsi qu'un régime transitoire applicable au fichier central.

Concernant la mise en conformité des fichiers autres que le fichier central, les auteurs ont choisi les délais du 6 mars 2023, respectivement au plus tard du 6 mars 2026, alors que ce sont ceux prévus à l'article 63 de la loi du 1er août 2018 pour la mise en conformité par rapport aux règles relatives à la journalisation. Comme des efforts de programmation devront donc être réalisés au plus tard pour ces dates, il s'avère opportun de prévoir les mêmes délais pour les autres adaptations à prévoir dans le cadre du présent projet de loi, qui exige des travaux considérables sur le plan technique, le recrutement de personnel hautement spécialisé et l'intervention de ressources externes.

Il convient également de préciser que la Police dispose de certaines banques de données spécialisées qui ont été acquises auprès de fournisseurs internationaux, tels les logiciels de comparaison des empreintes digitales ou d'empreintes génétiques, ou d'autres applications utilisées notamment par le Service de police judiciaire en matière de gestion et d'exploitation des traces trouvées sur les lieux du crime. Les fournisseurs doivent de toute façon adapter leurs logiciels au plus tard pour l'année 2026, il convient donc de fixer la même date pour la mise en conformité par rapport aux dispositions de la présente loi, afin d'éviter des coûts disproportionnés ou le risque de ne pas pouvoir effectuer les interventions nécessaires dans le délai fixé.

Concernant le fichier central, il est impossible de supprimer l'ancien fichier central à courte échéance et de migrer tout son contenu vers le nouveau fichier central. Par conséquent, un régime transitoire s'impose, prévu par les alinéas 3 à 7.

Ad article 8

L'entrée en vigueur des dispositions applicables à tous les fichiers ainsi que celles applicables au fichier central est prévue le 1er jour du sixième mois après la publication au Journal officiel du Grand-Duché de Luxembourg, afin de permettre à la Police d'entreprendre les mesures nécessaires à la mise en œuvre effective et complète du nouveau fichier central. Les dispositions relatives à la modification de l'article 43 de la loi sur la Police, la désignation du responsable du traitement, la suppression de l'accès du SRE, la modification des articles 509-1 et suivants du Code pénal ainsi que les dispositions relatives au régime transitoire du fichier central entrent en vigueur suivant les dispositions de l'article 4 de la loi du 23 décembre 2016 concernant le Journal officiel du Grand-Duché de Luxembourg.

*

TEXTES COORDONNES

Les modifications résultant du projet de loi sont indiquées en caractères gras et soulignés

LOI DU 18 JUILLET 2018

sur la Police grand-ducale et portant modification :

1° du Code de procédure pénale ;

2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ;

3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ;

4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ;

5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ;

et portant abrogation :

1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant

1. la loi modifiée du 23 juillet 1952 concernant l'organisation militaire ;

2. le code d'instruction criminelle ;

3. la loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ;

2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police

(Mém. A – 621 du 28 juillet 2018; doc. parl. 7045)

modifiée par:

Loi du 1er août 2018 (Mém. A – 689 du 16 août 2018; doc. parl. 7168; dir. (UE) 2016/680)

Loi du 15 décembre 2019 (Mém. A – 899 du 28 décembre 2019; doc. parl. 7418)

Loi du 29 juillet 2020 (Mém. A – 659 du 31 juillet 2020; doc. parl. 7543).

Chapitre 5 – Traitement de données à caractère personnel

Art. 43. ~~Dans l'exercice de leurs missions de police judiciaire et de police administrative, les membres de la Police ayant la qualité d'officier de police judiciaire ou d'officier de police administrative ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants :~~

~~1° le registre général des personnes physiques créé par la loi du 19 juin 2013 relative à l'identification des personnes physiques et le répertoire général créé par la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ;~~

~~2° le fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la Sécurité sociale, à l'exclusion de toutes données relatives à la santé ;~~

~~3° le fichier des étrangers exploité pour le compte du Service des étrangers du ministre ayant l'Immigration dans ses attributions ;~~

4° le fichier des demandeurs d'asile exploité pour le compte du Service des réfugiés du ministre ayant l'Immigration dans ses attributions ;

5° le fichier des demandeurs de visa exploité pour le compte du bureau des passeports, visas et légalisations du ministre ayant les Affaires étrangères dans ses attributions ;

6° le fichier des autorisations d'établissement exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions ;

7° le fichier des titulaires et demandeurs de permis de conduire exploité pour le compte du ministre ayant les Transports dans ses attributions ;

8° le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministre ayant les Transports dans ses attributions ;

9° le fichier des assujettis à la taxe sur la valeur ajoutée, exploité pour le compte de l'Administration de l'enregistrement et des domaines ;

10° le fichier des armes prohibées du ministre ayant la Justice dans ses attributions ;

11° le fichier des sociétés du registre de commerce et des sociétés.

Dans l'exercice de ces mêmes missions, les membres de la Police ayant la qualité d'agent de police judiciaire ou d'agent de police administrative ont accès direct, par un système informatique, aux fichiers visés aux points 1° à 8°, 10° et 11° de l'alinéa 1er. Il en est de même pour les membres du cadre civil de la Police, nommément désignés par le ministre sur proposition du directeur général de la Police grand-ducale, en fonction de leurs attributions spécifiques.

Les données à caractère personnel des fichiers accessibles en vertu des alinéas 1 et 2 sont déterminées par règlement grand-ducal.

Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que :

1° les membres de la Police visés aux alinéas 1 et 2 ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel, et

2° les informations relatives aux membres de la Police ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de trois ans, afin que le motif de la consultation puisse être retracé. Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation.

Seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées.

(Loi du 1er août 2018)

L'autorité de contrôle prévue à l'article 2, paragraphe 1er, point 15), lettre a), de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale contrôle et surveille le respect des conditions d'accès prévues par le présent article. Le rapport à transmettre au ministre ayant la Protection des données dans ses attributions, en exécution de l'article 10 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercée au titre du présent article.

(1) Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'officier ou d'agent de police judiciaire ou d'officier ou d'agent de police administrative ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants :

1° le registre général des personnes physiques créé par la loi du 19 juin 2013 relative à l'identification des personnes physiques et le répertoire général créé par la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ;

2° le fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la Sécurité sociale, à l'exclusion de toutes données relatives à la santé ;

3° le fichier des étrangers exploité pour le compte du Service des étrangers du ministre ayant l'Immigration dans ses attributions ;

4° le fichier des demandeurs d'asile exploité pour le compte du Service des réfugiés du ministre ayant l'Immigration dans ses attributions ;

5° le fichier des demandeurs de visa exploité pour le compte du bureau des passeports, visas et légalisations du ministre ayant les Affaires étrangères dans ses attributions ;

6° le fichier des autorisations d'établissement exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions ;

7° le fichier des titulaires et demandeurs de permis de conduire exploité pour le compte du ministre ayant les Transports dans ses attributions ;

8° le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministre ayant les Transports dans ses attributions ;

9° le fichier des armes prohibées du ministre ayant la Justice dans ses attributions.

(2) Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'officier de police judiciaire ou d'officier de police administrative ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants, s'ils font partie d'une entité de la Police dont les missions justifient cet accès ou figurent sur une liste agrée par le directeur général de la Police après avis du délégué à la protection des données de la Police :

1° le fichier des assujettis à la taxe sur la valeur ajoutée, exploité pour le compte de l'Administration de l'enregistrement et des domaines ;

2° le fichier des sociétés du registre de commerce et des sociétés ;

3° le registre foncier ;

4° le registre des bénéficiaires effectifs ;

5° le registre public des bâtiments de plaisance battant pavillon luxembourgeois ;

6° le système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg ;

7° le registre des fiducies et des trusts.

(3) Les membres du cadre civil de la Police, nommément désignés par le ministre sur proposition du directeur général de la Police grand-ducale, après avis du délégué à la protection des données de la Police, peuvent avoir accès aux fichiers prévus aux paragraphes (1) et (2) en fonction de leurs attributions spécifiques de support d'un officier ou agent de police judiciaire ou d'un officier ou agent de police administrative ou à des fins administratives.

(4) Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'agent de police judiciaire ou d'agent de police administrative nommément désignés par le directeur général de la Police grand-ducale, après avis du délégué à la protection des données de la Police, peuvent avoir accès aux fichiers prévus aux paragraphes (2).

(5) Les données à caractère personnel des fichiers accessibles en vertu des paragraphes (1) et (2) sont déterminées par règlement grand-ducal.

(6) Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que :

1° les membres de la Police visés aux paragraphes (1), (2) et (3) ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel ; et

2° les informations relatives aux membres de la Police ayant procédé à la consultation ainsi que les informations consultées, le motif de la consultation, ainsi que la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de cinq ans.

(7) Nonobstant les droits d'accès prévus aux paragraphes (1) à (4), les données à caractère personnel consultées doivent avoir un lien direct avec les motifs de consultation. Seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées.

(8) L'autorité de contrôle prévue à l'article 2, paragraphe 1er, point 15), lettre a), de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale contrôle et surveille le respect des conditions d'accès prévues par le présent article. Le rapport à transmettre au ministre ayant la protection des données dans ses attributions, en exécution de l'article 10 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercée au titre du présent article. »

Art. 43-1. (1) Sans préjudice de dispositions légales spécifiques, le présent article 43-1 s'applique à tous les fichiers que la Police gère en tant que responsable du traitement, conformément à l'article 1er de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

(2) Les fichiers de la Police peuvent contenir des données à caractère personnel relevant des catégories particulières prévues par l'article 9 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale dans la mesure où ces catégories particulières de données sont pertinentes et essentielles à l'aide de l'identification d'une personne, pour comprendre le contexte décrit dans un rapport ou procès-verbal établi par la Police et pour apprécier correctement les faits qui peuvent donner lieu à une infraction pénale ou à une mesure de police administrative au sens de la section 1ière du chapitre 2 de la présente loi ou en vertu d'une autre mission dont la Police est investie par la loi. Les données de ce type ont toujours un rapport avec d'autres données relatives à la personne concernée.

(3) La Police détermine des profils et des modalités d'accès et de traitement de données à caractère personnel sur la base :

1° du détail des informations concernées. La Police met en œuvre des règles spécifiques pour l'accès à ses rapports, procès-verbaux et autres pièces ;

2° du type du traitement de données, tels qu'une collecte, une modification, une consultation, une communication, un effacement ou une transmission de données ;

3° de l'appartenance à un service déterminé ou d'une unité au sein de la Police et de la fonction du membre de la Police ;

4° du motif d'accès. Si le motif d'accès ne découle pas incontestablement de l'affectation de l'agent au sein d'un service ou d'une unité de la Police, le motif d'accès doit indiquer la raison précise de la consultation. La Police détermine des motifs d'accès spécifiques selon le type de mission légale de la Police dans le cadre de laquelle un traitement de données est requis ;

5° de l'état de validation des données traitées ;

6° des règles spécifiques pour les données relatives à des mineurs qui prévoient que les rapports, procès-verbaux et autres pièces établis par la Police par rapport à un mineur ne peuvent être accédés que par :

a) les membres de la section « protection de la jeunesse » au sein du Service de police judiciaire ;

b) les officiers et agents de police judiciaire qui sont chargés d'une enquête par rapport au mineur concerné ou suite à une demande du service central d'assistance sociale (SCAS) du Parquet Général.

Dans le cas d'une demande de consultation d'un fichier par une personne autre que celle qui l'effectue, les journaux du fichier font mention de l'identité de la personne à l'origine de la demande et du motif de cette demande.

(4) La durée de conservation des données est définie par le responsable du traitement et ne sera en aucun cas supérieure à celles qui sont applicables au fichier central, sauf si une disposition légale spécifique prévoit une durée plus longue.

(5) Les données de journalisation collectées conformément à l'article 24 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à

caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont conservées pendant un délai de cinq ans.

Art. 43-2. (1) Dans le fichier central, la Police peut traiter les données à caractère personnel et informations relatives aux personnes qui ont fait l'objet d'un procès-verbal ou rapport dans le cadre de l'exécution d'une mission de police judiciaire, d'une mission de police administrative ou de toute autre mission dont la Police est investie par la loi.

Le fichier central comprend une partie active et une partie passive. La partie active contient les données auxquelles les membres de la Police ont besoin d'accéder dans le cadre de leurs missions légales conformément aux délais de conservations prévus aux paragraphes 9, 10, 11, 13 et 14. Après avoir atteint la durée de conservation maximale dans la partie active, les données collectées dans le cadre de l'exécution d'une mission de police judiciaire sont transférées dans la partie passive, à laquelle l'accès n'est justifié que pour les finalités prévues au paragraphe 19.

Le fichier central ne comporte pas les données relatives à des personnes qui ont commis une contravention si une loi spéciale permet d'arrêter les poursuites pénales par le paiement d'un avertissement taxé et que la personne concernée s'est acquittée de l'avertissement taxé dans le délai prévu par la loi.

(2) Les données à caractère personnel et informations sont traitées dans le fichier central pour les finalités suivantes :

1° la vérification des antécédents d'une personne dans le cadre d'une mission de police judiciaire, de police administrative ou dans le cadre d'une autre mission légale de la Police ;

2° l'appui aux enquêtes judiciaires par le biais d'analyses criminelles opérationnelles à la demande d'une autorité judiciaire ;

3° l'appui à la définition et à la réalisation de la politique de sécurité intérieure par le biais d'analyses criminelles stratégiques ;

4° l'exploitation des informations à des fins de recherches statistiques ;

5° l'identification des membres de la Police en charge du dossier.

(3) Les catégories de personnes concernées dont les données sont traitées dans le fichier central aux fins de police administrative et de toute autre mission dont la Police est investie par la loi, sont les personnes ayant fait l'objet d'une mesure de police ou ayant été citées dans un rapport établi par la Police dans le cadre de l'exécution de ses missions. Ces catégories comprennent :

1° les personnes ayant fait l'objet d'une mesure de police administrative prise par la Police au sens de la section 1ière du chapitre 2 de la présente loi ou sur base d'une loi spéciale ;

2° les personnes signalées ou recherchées par la Police afin que la Police puisse accomplir ses missions au sens de l'article 7 de la présente loi ;

3° les membres de la Police en charge du dossier.

(4) Les catégories de personnes dont les données sont traitées dans le fichier central aux fins de police judiciaire sont les suivantes :

1° les personnes suspectées d'avoir participé à une infraction pénale ;

2° les personnes reconnues coupables d'une infraction pénale ;

3° les personnes décédées de manière suspecte ;

4° les personnes disparues ;

5° les personnes signalées ou recherchées par la Police ;

6° les personnes évadées ou qui ont tenté de s'évader ;

7° les personnes qui exécutent une peine ;

8° les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;

9° les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures ;

10° les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale, ainsi que les contacts ou associés qui sont suspectés d'avoir l'intention de participer à ces infractions ou d'en avoir connaissance, ainsi que les personnes qui peuvent fournir des informations sur ces infractions pénales ;

11° les membres de la Police en charge du dossier.

Les personnes visées au point 10° ne peuvent faire l'objet d'une inscription dans le fichier central que :

1° par les officiers de police judiciaire du Service de police judiciaire dans les matières qui relèvent des attributions de la section à laquelle ils sont affectés ;

2° si la fiabilité de la source et de l'information est évaluée suivant un code d'évaluation préalablement défini qui tient compte de la pertinence de la source et de l'information fournie dans le contexte de l'évolution de la criminalité et des phénomènes criminels pertinents ; et

3° avec l'accord du procureur général d'Etat ou du membre de son parquet désigné à cet effet si ces données concernent un mineur.

(5) Une consultation du fichier central pour un motif autre qu'un motif de police judiciaire ne donne pas accès aux données à caractère personnel des personnes prévues à l'article 43-2, paragraphe (4), points 8°, 9° et 10°, sauf pour les consultations administratives qui relèvent de la police des étrangers qui donnent accès aux points 8° et 9°.

Une consultation du fichier central pour un motif de police judiciaire ne donne pas accès aux données à caractère personnel des personnes prévues à l'article 43-2, paragraphe (4), alinéa 1er, point 10° à l'agent consultant, mais génère un avertissement auprès des officiers de police judiciaire en charge de l'information. Il appartient aux agents en charge de l'information d'évaluer l'utilité de prendre contact avec l'agent consultant.

Par dérogation à l'alinéa précédent, les officiers et les agents de police judiciaire du Service de police judiciaire ont accès direct à ces données, sauf si les agents qui sont en charge de l'information ont limité l'accès à une ou plusieurs sections du Service de police judiciaire.

Les agents en charge de l'information peuvent autoriser l'accès direct aux informations à l'égard des personnes auxquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale. Dans ce cas, ces informations sont traitées comme celles qui relèvent des catégories prévues au paragraphe (4), alinéa 1er, point 1°.

(6) Pour l'exercice de leurs fonctions, un accès direct au fichier central peut être accordé par le responsable du traitement aux fonctionnaires de l'Administration des douanes et accises ayant la qualité d'officier de police judiciaire et nommément désignés par le directeur de l'Administration des douanes et accises.

Pour l'exercice de leurs missions prévues aux articles 4, 8 et 9 de la loi modifiée du 18 juillet 2018 sur l'Inspection générale de la Police, un accès direct au fichier central peut être accordé par le responsable du traitement à l'Inspecteur général de la Police, à l'Inspecteur général adjoint de la Police et aux membres du cadre policier de l'Inspection générale de la Police.

(7) Dans le respect des règles d'accès déterminées en vertu de l'article 43-1, paragraphe (3) de la présente loi, le fichier central permet aux officiers et agents de police judiciaire et de police administrative, ainsi qu'au membres du personnel civil nommément désignés par le responsable du traitement, de déterminer si une personne y figure. Elle permet également à visionner les informations et données à caractère personnel principales par rapport à cette personne et, le cas échéant, un résumé sommaire de faits dans lesquels la personne est impliquée. Les procès-verbaux et rapports dont la personne fait l'objet sont également accessibles en fonction des droits d'accès et des motifs de la consultation.

Les informations et données à caractère personnel principales par rapport aux personnes visées aux paragraphes (3) et (4) peuvent contenir les données suivantes si elles sont disponibles pour les personnes physiques :

1° le(s) nom(s), prénom(s), alias et surnoms ;

2° la date et le lieu de naissance ;

3° la ou les nationalités ou le statut d'apatride ;

4° l'état civil ;

5° la date de décès ;

6° le numéro d'identification national ou, le cas échéant, un numéro équivalent ;

7° le domicile, la résidence habituelle ou la dernière adresse connue ;

8° le numéro de la carte d'identité et/ou du passeport ou de tout autre document officiel ;

9° le numéro du téléphone et les données y afférentes et, le cas échéant, une adresse électronique ;

10° le signalement descriptif, comprenant les signes corporels inaltérables permettant d'identifier la personne, y compris les photographies et, le cas échéant, les empreintes digitales.

Dans le cas d'une personne morale, les informations et données à caractère personnel principales peuvent contenir les données suivantes si elles sont disponibles :

1° la dénomination sociale et, le cas échéant, la dénomination commerciale si elle est différente de la dénomination sociale ;

2° le(s) nom(s), prénom(s), alias et surnoms des dirigeants et des bénéficiaires économiques ainsi que leur date et lieu de naissance et leur numéro d'identification national ou, le cas échéant, un numéro équivalent ;

3° la date et le lieu de constitution ;

4° l'adresse du siège social et les adresses d'exploitation ;

5° le numéro du téléphone et les données y afférentes et, le cas échéant, une adresse électronique.

(8) Les données à caractère personnel et les informations prévues aux paragraphes (3) et (4) sont transmises au fichier central si l'enquête est terminée, ou si l'autorité judiciaire compétente a autorisé la transmission conformément à la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière.

(9) En présence d'une décision de condamnation coulée en force de chose jugée, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour crime ou délit adressés aux autorités judiciaires sont transférées dans la partie passive du fichier central dès que la Police est informée que la décision de condamnation est supprimée du casier judiciaire de toutes les personnes condamnées.

Si la réhabilitation ne concerne pas toutes les personnes impliquées dans la poursuite pénale de l'affaire visée, les informations et données à caractère personnel de la personne réhabilitée sont maintenues dans la partie active. Dans ce cas, la personne réhabilitée dans l'affaire visée ne peut plus être recherchée dans la partie active par le biais de ses données à caractère personnel à partir de la suppression de la condamnation du casier judiciaire.

Dès qu'une condamnation est prononcée dans une affaire, les victimes et témoins ne peuvent plus être recherchés dans la partie active par le biais de leurs données à caractère personnel, sauf si une disjonction des poursuites a été prononcée dans l'affaire visée et que la recherche de personnes suspectées d'avoir participé à l'infraction continue.

(10) En présence d'une décision d'acquittement coulée en force de chose jugée, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour crime ou délit adressés aux autorités judiciaires sont transférées dans la partie passive du fichier central dès que la Police est informée de la décision d'acquittement, sauf si le Procureur d'Etat ordonne leur maintien.

Si l'acquittement ne concerne pas toutes les personnes impliquées dans la poursuite pénale de l'affaire visée ou si après l'acquittement d'un prévenu l'enquête est reprise pour rechercher l'auteur de l'infraction, les informations et données à caractère personnel de la personne acquittée sont maintenues dans la partie active. Dans ce cas, la personne acquittée dans l'affaire visée ne peut plus être recherchée dans la partie active par le biais de ses données à caractère personnel, sauf si la personne concernée a fait l'objet d'une audition comme témoin dans une phase initiale de l'enquête, dans quel cas elle reste liée à l'affaire sous ces statuts respectifs.

Si l'enquête est reprise suite à un acquittement ou si l'enquête continue suite à une disjonction des poursuites, les données relatives aux victimes et témoins sont maintenues dans la partie active.

(11) En l'absence de décision coulée en force de chose jugée d'une juridiction de jugement, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour crime ou délit adressés aux autorités judiciaires, sont conservées dans la partie active du fichier central jusqu'à ce que le dossier relatif à la poursuite pénale soit archivé au sein du traitement, dit chaîne pénale du ministère public. Les informations et données à caractère personnel sont transférées dans la partie passive du fichier central dès que la Police est informée de l'archivage au sein du traitement, dit chaîne pénale, du ministère public.

(12) Les décisions de condamnation, d'acquittement, de non-lieu ou de classement sans suites sont mentionnées dans le fichier central.

(13) Le procureur d'Etat peut à tout moment, d'office ou à la demande de la personne concernée, soit ordonner le transfert des informations, données à caractère personnel, procès-verbaux ou rapports relevant d'une mission de police judiciaire dans la partie passive du fichier central, soit ordonner que la personne concernée ne puisse plus être recherchée par le biais des données à caractère personnel. La décision est communiquée par écrit à la Police et fait l'objet d'une mention dans le dossier en question. Le procureur d'État avise la personne concernée des suites qu'il convient de donner aux demandes qui lui sont adressées.

Les décisions du Procureur d'Etat visées à l'alinéa précédent sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé ou si des raisons objectives ne justifient plus leur maintien.

Les décisions du procureur d'Etat sont susceptibles de recours devant le Président du tribunal d'arrondissement compétent en la matière.

(14) Par dérogation aux paragraphes 9, 10 et 11, les informations et données à caractère personnel sont transférées dans la partie passive après vingt ans pour les rapports rédigés dans le contexte d'une demande d'entraide judiciaire internationale.

Les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des documents qui relèvent de la coopération policière internationale ou dans des rapports aux autorités judiciaires qui n'ont pas comme objet la constatation d'une infraction pénale sont transférées dans la partie passive ensemble avec les procès-verbaux ou rapports élaborés dans le cadre de l'enquête à laquelle ils se rapportent. Si ces rapports ne concernent pas une enquête en cours ou une infraction déterminée, le délai de conservation prévu au paragraphe 15, alinéa 1er est applicable.

Les informations et données à caractère personnel contenues dans le fichier central qui relèvent des personnes visées à l'article 43-2, paragraphe (4), alinéa 1er, point 10° sont transférées dans la partie passive un an après leur enregistrement dans la partie active du fichier central. Ce délai peut être prolongé d'une année supplémentaire sur décision motivée de l'officier de police judiciaire en charge de l'information dans le fichier central. Si l'information se révèle être inexacte, elle est immédiatement supprimée. Seul l'officier de police judiciaire en charge de l'information peut la supprimer.

(15) Les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des rapports rédigés dans le cadre d'une mission de police administrative ou dans le cadre d'une mission administrative dont la Police est investie par la loi, sont supprimées au plus tard après une période de dix ans après leur enregistrement dans le fichier central. La Police peut arrêter des délais de conservation plus courts par type de rapport au sens de ce paragraphe, auquel cas elle tient un relevé dans lequel les délais spécifiques sont indiqués.

Les informations et données à caractère personnel contenues dans le fichier central relatives à des personnes mineures en fugue sont effacées du fichier central lorsque la personne a atteint l'âge de dix-huit ans.

(16) Les informations et données à caractère personnel contenues dans la partie passive du fichier central, et le cas échéant dans la partie passive des fichiers particuliers établis conformément à l'article 43-1, peuvent être retransmises dans la partie active pour les raisons suivantes :

1° les enquêtes sont reprises pour des infractions pénales qui ne sont pas encore prescrites ;

2° il s'agit d'enquêtes relatives à des faits dénoncés à des autorités judiciaires d'autres États ;

3° il s'agit de faits qui relèvent d'une décision d'enquête européenne ou d'une commission rogatoire internationale.

Une retransmission dans la partie active du traitement, dit chaîne pénale, du ministère public donne lieu à une retransmission dans la partie active du fichier central. Les informations et données à caractère personnel sont de nouveau transférées dans la partie passive du fichier central dès que la Police est informée de l'archivage au sein du traitement, dit chaîne pénale, du ministère public.

(17) Sans préjudice des dispositions relatives à l'archivage pour des raisons historiques, les informations et données à caractère personnel sont supprimées au plus tard trente ans après leur transfert dans la partie passive.

Par dérogation à l'alinéa qui précède, les informations et données à caractère personnel contenues dans le fichier central qui relèvent des personnes visées à l'article 43-2, paragraphe (4), alinéa 1er, point 10° sont supprimées trois ans après leur transfert dans la partie passive.

Par dérogation à l'alinéa 1er, les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour contraventions adressés aux autorités judiciaires, sont supprimées cinq ans après l'établissement du procès-verbal ou du rapport.

Les autorités judiciaires compétentes peuvent faire prolonger la durée de conservation dans la partie passive en raison d'une demande de révision en cours. La décision est communiquée par écrit à la Police et fait l'objet d'une mention dans le dossier en question.

(18) Au plus tard au moment du transfert dans la partie passive du fichier central des informations et données à caractère personnel relevant d'une mission de police judiciaire, les informations et données à caractère personnel en question qui se trouvent dans d'autres fichiers doivent être supprimées dans ceux-ci, sauf si ces fichiers sont régis par une disposition légale spécifique qui prévoit une durée de conservation différente.

Par dérogation à l'alinéa précédent, les informations et données à caractère personnel contenues dans d'autres fichiers dans un format qui ne peut pas être géré par le fichier central peuvent être archivées dans le fichier particulier s'il dispose d'une possibilité d'archivage. Les durées d'archivage et les conditions d'accès sont les mêmes que celles prévues pour la partie passive du fichier central.

Par dérogation à l'alinéa 1er, l'obligation de suppression des informations et données à caractère personnel contenues dans d'autres fichiers au moment du transfert des informations dans la partie passive du fichier central ne s'applique pas aux informations et données à caractère personnel relatives à des traces prélevées dans le cadre d'enquêtes où les auteurs des faits sont restés inconnus. Les durées de conservation sont les mêmes que celles prévues pour la partie passive du fichier central.

(19) L'accès aux informations et données à caractère personnel contenues dans la partie passive du fichier central, et le cas échéant dans la partie passive des fichiers particuliers établis conformément à l'article 43-1, peut être effectué pour les seules finalités suivantes :

1° la prise de connaissance des informations dans le cadre d'une enquête en cours relative à un crime ou un délit ;

2° la prise de connaissance des informations dans le cadre d'une demande en révision conformément aux articles 443 et suivants du Code de procédure pénale.

La consultation des informations et données à caractère personnel contenues dans la partie passive du fichier central pour une de ces finalités n'est possible qu'avec l'accord du procureur

général d'Etat ou des membres de son parquet désignés à cet effet ou, pour la finalité sous 1°, sur demande du juge d'instruction en charge de l'instruction préparatoire.

Le procureur général d'État peut autoriser l'accès aux informations et données à caractère personnel contenues dans la partie passive du fichier central à des officiers et agents de police judiciaire nommément désignées du Service de police judiciaire ou aux membres de certaines subdivisions du Service de police judiciaire pendant une période maximale de cinq ans renouvelable.

Art. 43-3. La Police grand-ducale a la qualité de responsable du traitement des traitements de données à caractère personnel effectués par la Police.

*

LOI DU 5 JUILLET 2016

1. portant réorganisation du Service de renseignement de l'Etat ;

2. modifiant

– le Code d'instruction criminelle,

– la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, et

– la loi du 25 mars 2015 fixant le régime des traitements et les conditions d'avancement des fonctionnaires de l'Etat,

(Mém. A – 129 du 15 juillet 2016, p. 2244; doc. parl. 6675)

modifiée par:

Loi du 1er août 2018 - protection des personnes physiques (Mém. A – 689 du 16 août 2018; doc. parl. 7168; dir. (UE) 2016/680)

Loi du 1er août 2018 - traitement des données (Mém. A – 690 du 16 août 2018; doc. parl. 7151; dir. (UE) 2016/681)

Loi du 10 août 2018 (Mém. A – 704 du 21 août 2018; doc. parl. 7281)

Loi du 25 mars 2020 (Mém. A – 193 du 26 mars 2020; doc. parl. 7512 ; dir. (UE) 2019/878 ; dir (UE) 2018/843 et dir. (UE) 2019/2034)

Chapitre 3 – De la collecte et du traitement des renseignements

Art. 9. – Coopération avec les instances nationales et internationales

(1) Le SRE veille à assurer une coopération efficace avec les autorités judiciaires, les services de la police grand-ducale et les administrations.

(2) Le SRE communique dans les meilleurs délais les renseignements collectés dans le cadre de ses missions aux autorités judiciaires, aux services de la police grand-ducale et aux administrations dans la mesure où ces renseignements paraissent utiles à l'accomplissement de leurs missions respectives.

(3) Les services de la police grand-ducale et les administrations communiquent au SRE les renseignements susceptibles d'avoir un rapport avec ses missions définies à l'article 3.

Dans le cas où le SRE désire obtenir des informations des services de la police grand-ducale et des administrations, le directeur du SRE leur adresse une demande écrite. Les services de la police grand-ducale et les administrations répondent par écrit et par la voie hiérarchique.

Sans préjudice de l'article 8 du Code d'instruction criminelle, les autorités judiciaires peuvent communiquer au SRE les informations et renseignements susceptibles d'avoir un rapport avec ses missions définies à l'article 3.

(4) Le SRE assure la coopération avec les organismes de renseignement et de sécurité étrangers, lorsqu'il s'agit de sauvegarder la sécurité extérieure et la sécurité nationale du Grand-Duché de

Luxembourg, ou lorsque ces services relèvent d'États ou d'organisations internationales envers lesquels le Grand-Duché de Luxembourg se trouve engagé par un traité portant sur la coopération réciproque en matière de sécurité extérieure ou de sécurité nationale.

(Loi du 1er août 2018 – protection des personnes physiques)

Sous réserve des conditions définies à l'alinéa 1er, le SRE peut échanger directement des données à caractère personnel avec des services de renseignement étrangers, y compris au moyen d'installations communes de transmission, conformément aux articles 34 et 38 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 10. – Accès aux renseignements

(Loi du 1er août 2018 – protection des personnes physiques)

(1) Le SRE procède au traitement de données à caractère personnel qui sont nécessaires à l'accomplissement de ses missions légales qui est effectué conformément aux dispositions de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Le traitement s'effectue conformément à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Il fait l'objet d'un règlement grand-ducal prévu à l'article 17, paragraphe 1er, de la loi précitée du 2 août 2002.

Tout accès aux données s'exerce en conformité avec le paragraphe 2, alinéa 5 du même article 17.

(2) Dans le cadre de l'exercice de sa mission, le SRE a accès direct, par un système informatique, aux traitements de données à caractère personnel suivants :

a) le registre national des personnes physiques créé par la loi du 19 juin 2013 relative à l'identification des personnes physiques;

b) le fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la sécurité sociale, à l'exclusion de toutes données relatives à la santé;

c) le fichier des étrangers exploité pour le compte du service des étrangers du ministre ayant l'Immigration dans ses attributions;

d) le fichier des demandeurs de visa exploité pour le compte du bureau des passeports, visas et légalisations du ministre ayant les Affaires étrangères dans ses attributions;

e) le fichier des autorisations d'établissement exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions;

f) le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministère ayant le Transport dans ses attributions;

g) le fichier des armes prohibées du ministre ayant la Justice dans ses attributions;

ainsi qu'aux systèmes de traitements de données suivants:

~~**h) la partie «recherche» de la banque de données nominatives de police générale.**~~

Le SRE peut s'adresser par écrit au procureur général d'État pour obtenir la communication du bulletin N°2 du casier judiciaire.

(Loi du 1er août 2018 – protection des personnes physiques)

Le SRE transmet sur une base trimestrielle la liste de ses demandes de délivrance et les motifs de ces demandes à l'autorité de contrôle judiciaire prévue à l'article 40 de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

(3) *(Loi du 1er août 2018 – protection des personnes physiques)* Le directeur est responsable du traitement des données visées aux paragraphes 1er et 2. Il désigne un chargé de la protection des données qui est compétent sous son autorité de l'application conforme de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en

matière pénale ainsi qu'en matière de sécurité nationale et de la mise en œuvre des mesures de sécurité des traitements auxquels procède le SRE.

Le chargé de la protection des données veille à la mise en place des moyens techniques permettant de rechercher l'ensemble des interventions relatives à l'accès aux banques de données prévues au paragraphe 2.

Tout traitement des données reprises dans les banques et fichiers de données à caractère personnel qui sont gérés par le SRE ou auxquels le SRE a accès ainsi que toute consultation de ces données ne peut avoir lieu que pour un motif précis qui doit être indiqué pour chaque traitement ou consultation avec l'identifiant numérique personnel de la personne qui y a procédé.

La date et l'heure de tout traitement ou consultation ainsi que l'identité de la personne qui y a procédé doivent pouvoir être retracées par un système informatique.

Art. 11. – Protection de l'identité des sources humaines

(1) Il est interdit à tout agent du SRE de divulguer l'identité d'une source humaine du SRE. Une personne qui a pris connaissance d'une information permettant d'identifier une source humaine du SRE est soumise à l'interdiction de l'alinéa 1.

(2) Les autorités judiciaires, la police grand-ducale et les autres administrations ne peuvent pas ordonner ou prendre des mesures qui auraient pour objet ou effet de porter atteinte à l'interdiction du paragraphe 1er.

(3) À la demande du ministère public ou du juge la protection des sources peut toutefois être levée à l'égard des autorités judiciaires sur décision d'un vice-président de la Cour supérieure de justice, à condition que cette levée n'entrave pas les actions en cours du SRE et qu'elle ne présente pas un danger pour une personne physique.

(4) Cette disposition ne s'applique ni aux renseignements fournis par un service étranger du renseignement ni aux renseignements qui, de par leur nature ou leur contenu, pourraient révéler l'identité d'une source humaine de ce service, sauf si celui-ci marque son accord avec la communication du renseignement. Le magistrat visé au paragraphe 3 vérifie l'origine étrangère des renseignements en question à la demande du ministère public ou du juge.

(5) Si des renseignements permettant d'identifier une source humaine ont été obtenus à l'occasion d'une procédure qui n'avait pas pour but de découvrir l'identité d'une source du SRE, ces données ne peuvent pas être utilisées comme preuve dans le cadre d'une action en justice, sauf

a) dans le cas où une telle utilisation des renseignements ne divulgue pas l'identité de la source, ou

b) dans les cas visés au paragraphe 3.

Art. 12. – Témoignage en justice

(1) L'agent du SRE sous la responsabilité duquel un moyen ou une mesure de recherche opérationnelle déterminés aux articles 4 à 8 a été mis en œuvre peut seul être entendu en qualité de témoin sur une opération.

(2) S'il ressort du dossier que la personne inculpée ou comparaissant devant la juridiction de jugement est directement mise en cause par des constatations effectuées par un agent du SRE ayant personnellement mis en œuvre un des moyens ou une des mesures de recherche opérationnelle visé au paragraphe 1er, cette personne peut demander à être confrontée avec cet agent du SRE par l'intermédiaire d'un dispositif technique permettant l'audition du témoin à distance ou à faire interroger ce témoin par son avocat par ce même moyen. L'identité de l'agent du SRE est protégée. La voix du témoin est alors rendue non identifiable par des procédés techniques appropriés.

Les questions posées à l'agent du SRE à l'occasion de cette confrontation ne doivent pas avoir pour objet ni pour effet de révéler, directement ou indirectement, sa véritable identité.

Aucune condamnation ne peut être prononcée sur le seul fondement des déclarations faites par l'agent du SRE au sens du présent paragraphe.

Art. 13. – Saisies et perquisitions de données et de matériel du SRE

(1) Lorsqu'une saisie ou une perquisition est effectuée dans un lieu où le SRE exerce ses missions, le directeur du SRE est invité à y assister ou à se faire représenter. Le directeur du SRE en informe sans délai le délégué au SRE.

(2) Si le directeur du SRE ou son représentant estime que la saisie de données ou de matériels classifiés est de nature à présenter un des risques prévus au paragraphe 3 de l'article 11 ou concerne les renseignements visés au paragraphe 4 de l'article 11 ou les informations visées aux paragraphes 1er et 2 de l'article 26, il demande la mise sous scellés des données et matériels concernés, munis du sceau du juge d'instruction et conservés en lieu sûr par celui-ci.

Le juge d'instruction peut demander la levée des scellés à un vice-président de la Cour supérieure de justice. Celui-ci prend sa décision après avoir demandé l'avis du directeur du SRE. Si le vice-président estime que le versement au dossier judiciaire de tout ou partie des données et matériels sous scellés permettrait de révéler l'identité d'une source humaine du SRE, il ordonne la restitution au SRE des données et matériels concernés. Les autres données et matériels sous scellés pour lesquels le vice-président estime que ce risque n'est pas donné, sont versés au dossier judiciaire.

(3) Lorsque la saisie porte sur des dossiers pour lesquels le SRE détient des renseignements provenant de services partenaires ou d'organisations internationales, le directeur du SRE ou son représentant demande également la mise sous scellé des données et matériels concernés, munis du sceau du juge, à l'origine de la saisie, et conservés en lieu sûr par celui-ci.

Un vice-président de la Cour supérieure de justice vérifie à la demande du juge l'origine étrangère des renseignements en question.

Si l'origine étrangère est vérifiée, le juge peut demander au SRE de solliciter, auprès du service partenaire ou de l'organisation internationale concernée, l'autorisation de communication aux autorités judiciaires. En cas d'accord, le scellé est levé et les données et matériels sont intégrés au dossier judiciaire. En cas de refus de l'accord, le scellé est levé et les données et matériels sont restitués au SRE.

Si l'origine étrangère n'est pas vérifiée, le scellé est levé conformément à la procédure prévue au paragraphe 2, alinéa 2, et les données et matériels sont versés au dossier judiciaire.

(4) Si lors d'une saisie ou d'une perquisition effectuée en tout autre lieu, des données ou du matériel classifiés sont découverts qui risquent de permettre de révéler l'identité d'une source humaine du SRE, le directeur du SRE en est informé sans délai. Si le directeur ou son représentant estime que le risque en question est donné, il est procédé conformément aux paragraphes 2 et 3.

Art. 14. – Armes de service

Le directeur du SRE peut autoriser des membres du SRE qui, en raison de leur engagement opérationnel, sont exposés à un risque physique personnel et direct, à solliciter auprès du ministre ayant la Justice dans ses attributions l'autorisation de porter, pour des raisons de légitime défense, une arme de service.

*

CODE PENAL

Section VII. – De certaines infractions en matière informatique
et de systèmes de traitement ou de transmission de données

(L. 15 juillet 1993)

Art. 509-1. (L. 14 août 2000) Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Sera puni des mêmes peines, quiconque, disposant d'une autorisation d'accès à tout ou partie d'un système de traitement ou de transmission automatisé ou non-automatisé de données à caractère personnel, y effectue un traitement de données à caractère personnel pour des finalités

autres que celles pour lesquelles l'autorisation d'accès a été accordée, y inclus le fait de porter à la connaissance d'un tiers non autorisé les données à caractère personnel ainsi obtenues.

Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros.

Art. 509-2. (L. 15 juillet 1993) Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé **ou non-automatisé** de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

Art. 509-3. (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé **ou non-automatisé** ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

(L. 18 juillet 2014) Sera puni des mêmes peines celui qui aura intentionnellement et au mépris des droits d'autrui, intercepté des données lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système de traitement ou de transmission automatisé **ou non-automatisé** de données.

Art. 509-4. (L. 10 novembre 2006) Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros.

Alinéa abrogé (L. 18 juillet 2014)

Art. 509-5. (L. 18 juillet 2014) Sera puni de 4 mois à cinq ans d'emprisonnement et d'une amende de 1.250 euros à 30.000 euros quiconque aura, dans une intention frauduleuse, produit, vendu, obtenu, détenu, importé, diffusé ou mis à disposition,

– un dispositif informatique destiné à commettre l'une des infractions visées aux articles 509-1 à 509-4; ou
– toute clef électronique permettant d'accéder, au mépris des droits d'autrui, à tout ou à partie d'un système de traitement ou de transmission automatisé de données.

Art. 509-6. (L. 15 juillet 1993) La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même.

Art. 509-7. (L. 15 juillet 1993) Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

*

FICHE FINANCIERE

Conformément à l'article 79 de la loi modifiée du 8 juin 1999 portant sur le budget, la comptabilité et la trésorerie de l'Etat, Monsieur le Ministre de la Sécurité intérieure déclare que le présent projet de loi est susceptible de grever le budget de l'Etat.

L'projet de loi prévoit de centraliser dans le fichier central tous les procès-verbaux, rapports, autres documents, informations et données à caractère personnel relatives aux personnes qui ont fait l'objet d'un tel procès-verbal ou rapport dans le cadre de l'exécution d'une mission de police judiciaire, de police administrative ou de toute autre mission dont la Police est investie par la loi. Il réglemente à la fois les catégories de personnes concernées ainsi que les catégories de données qui peuvent être traitées

dans le fichier central. D'autres dispositions traitent des durées de conservation des données à caractère personnel, ce qui implique un retour d'informations automatisé des suites réservées aux procès-verbaux par les autorités judicaires entre le fichier central et le traitement, dit chaîne pénale (JUCHA) du ministère public, ainsi que les profils et modalités d'accès à ces données. Le projet de loi a pour effet que d'importants travaux d'inventaires, d'études, de conceptualisation et de programmation doivent être entrepris afin de tenir compte des nouveaux concepts, ainsi qu'une catégorisation des données et des documents plus poussés. Afin de répondre à ces nouvelles exigences, une grande partie des fichiers de la Police, les applications ainsi que les flux de données doivent être complètement revus et redéveloppés. Une nouvelle architecture des données et une nouvelle architecture logicielle sont nécessaires.

Le projet de loi prévoit deux échéanciers de 2023 et de 2026 pour une mise en conformité. Vu la complexité et l'ampleur des travaux à réaliser, il est préconisé d'anticiper les travaux et de libérer les fonds nécessaires à partir de l'année 2021.

L'estimation des coûts s'étale sur la période de 2021 à 2026. Les calculs comprennent une assistance à la maîtrise d'ouvrage, des études et analyses, ainsi que l'établissement des cahiers de charge. Il s'y ajoutent les coûts pour le développement et la réalisation, ainsi que des frais liés à la maintenance évolutive, les acquisitions et frais liés à la formation.

Assistance à la maitrise d'ouvrage	*2021*	*2022*	*2023*	*2024*	*2025*	*2026*	*Total*
Total Budget Gestion de projet	- €	220 000 €	220 000 €	220 000 €	220 000 €	- €	**880 000** €
Total Budget Etudes et CdC	495 000 €	1 188 000 €	792 000 €	- €	- €	- €	**2 475 000** €
Total Budget Réalisations	374 000 €	2 618 000 €	2 618 000 €	2 618 000 €	2 244 000 €	- €	**10 472 000** €
Total Budget maint. év. et corr.	- €	93 500 €	280 500 €	561 000 €	935 000 €	748 000 €	**2 618 000** €
Total Budget acquisitions	- €	- €	1 000 000 €	1 250 000 €	750 000 €	- €	**3 000 000** €
Total Budget formations	- €	220 000 €	440 000 €	440 000 €	440 000 €	220 000 €	**1 760 000** €
Grand Total	**869 000.00** €	**4 119 500.00** €	**4 910 500.00** €	**4 649 000.00** €	**4 149 000.00** €	**748 000.00** €	**21 205 000.00** €

Besoins en recrutement interne	*2021*	*2022*	*2023*	*2024*	*2025*	*2026*	*Total*
Gestion de projets	1						**1**
Etudes et cahiers des charges	1						**1**
Réalisations	1	2	2				**5**
Maintenance évolutive et corr.		1	1	1			**3**
Formations		1					**1**
Grand-Total	**3**	**4**	**3**	**1**	**0**	**0**	**11**

Détail :

Assistance à la maitrise d'ouvrage	*2021*	*2022*	*2023*	*2024*	*2025*	*2026*	
Gestion de projets	**0**	**220**	**220**	**220**	**220**	**0**	**880**
ETP externes	0	1	1	1	1	0	4
Ress. internes J/H	*220*	*220*	*220*	*220*	*220*	*220*	*1320*
ETP internes	***1***	*1*	*1*	*1*	*1*	*1*	*6*
Total J/H	220	440	440	440	440	220	1980
Total Budget Gestion de projets	**- €**	**220 000 €**	**220 000 €**	**220 000 €**	**220 000 €**	**- €**	**880 000 €**
Etudes et cahiers des charges							
Etudes J/H	**440**	**220**	**0**	**0**	**0**	**0**	**660**
ETP externes	2	1	0	0	0	0	3
Ress. internes J/H	*220*	*440*	*0*	*440*	*440*	*440*	*1980*
ETP internes	***1***	*2*	*0*	*2*	*2*	*2*	*9*
Total J/H Arch. Entr.	660	660	0	440	440	440	2640
Budget Etudes	**396 000 €**	**198 000 €**	**- €**	**- €**	**- €**	**- €**	**594 000 €**

	2021	*2022*	*2023*	*2024*	*2025*	*2026*	
Cahier des charges J/H	**110**	**1100**	**880**	**0**	**0**	**0**	**2090**
ETP externes	0.5	5	4	0	0	0	9.5
Ress. internes J/H	*110*	*220*	*440*	*440*	*440*	*440*	*2090*
ETP internes	*0*	***1***	*1*	*1*	*1*	*1*	*9.5*
Total J/H analyses	220	1320	1320	440	440	440	4180
Budget Cahier des charges (CdC)	**88 000 €**	**990 000 €**	**792 000 €**	**- €**	**- €**	**- €**	**1 881 000 €**
Total J/H externes	***550***	***1320***	***880***	***0***	***0***	***0***	***2750***
Total ETP externes	***2.5***	***6***	***4***	***0***	***0***	***0***	***12.5***
Total Budget Etudes et CdC	**495 000 €**	**1 188 000 €**	**792 000 €**	**- €**	**- €**	**- €**	**2 475 000 €**
Réalisations							
Analyses dét. et Dével. J/H	**440**	**3080**	**3080**	**3080**	**2640**	**0**	**12320**
ETP	2	14	14	14	12	0	56
Ress. internes J/H	*0*	*440*	*880*	*880*	*880*	*0*	*3080*
ETP internes	***1***	***2***	***4***	*4*	*3*	*0*	*14*
Total J/H réalisations	440	3520	3960	3960	3520	0	15400
Total Budget Réalisations	**374 000 €**	**2 618 000 €**	**2 618 000 €**	**2 618 000 €**	**2 244 000 €**	**- €**	**10 472 000 €**
Maintenance évolutive et corr.							
Maintenance évolutive et corr. J/H	**0**	**110**	**330**	**660**	**110**	**880**	**3080**
ETP	0	0.5	1.5	3	5	4	14
Ress. internes	*0*	*110*	*440*	*660*	*880*	*1540*	*3630*
ETP internes	*0*	***1***	***2***	***3***	*4*	*7*	*16.5*
Total Budget maint. év. et corr.	**- €**	**93 500 €**	**280 500 €**	**561 000 €**	**935 000 €**	**748 000 €**	**2 618 000 €**
Acquisitions							
Matériel et installations	-	-	1 000 000	1 250 000	750 000	-	3 000 000
Total Budget acquisitions	**- €**	**- €**	**1 000 000 €**	**1 250 000 €**	**750 000 €**	**- €**	**3 000 000 €**
Formations							
Elaboration de turoriels interactifs	-	220	440	440	440	220	1 760
ETP	0	1	2	2	2	1	8
Ress. internes	*0*	*220*	*220*	*220*	*220*	*220*	*110*
ETP internes	*0*	***1***	*1*	*1*	*1*	*1*	*5*
Total Budget formations	**- €**	**220 000 €**	**440 000 €**	**440 000 €**	**440 000 €**	**220 000 €**	**1 760 000 €**
Grand-Total	**869 000.00 €**	**4 119 500 €**	**4 910 500.00 €**	**4 649 000.00 €**	**4 149 000.00 €**	**748 000.00 €**	**21 205 000.00 €**
Total ETP externes	**4.5**	**22.5**	**22.5**	**20**	**20**	**5**	
Total ETP internes	**2**	**7**	**8**	**11**	**11**	**11**	

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet :	**Projet de loi portant modification** **1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ;** **2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; et** **3° du Code pénal.**
Ministère initiateur :	**Ministère de la Sécurité intérieure**
Auteur(s) :	**Barbara Ujlaki**
Téléphone :	**247-74612**
Courriel :	**barbara.ujlaki@msi.etat.lu**
Objectif(s) du projet :	**Encadrer le traitement des données à caractère personnel dans les fichiers de la Police grand-ducale.**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :	
Date :	**09/12/2020**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s) : Oui ☒ Non ☐
   Si oui, laquelle/lesquelles : Ministère de la Justice
   Remarques/Observations : Un groupe de suivi avait été constitué en octobre 2019, qui est réuni au moins une fois par mois, afin de suivre la mise en oeuvre des recommandations de la CNPD et de l'IGP, et afin de discuter sur les travaux relatifs au projet de loi sous examen. Le groupe de suivi est composé par des représentants du Ministère de la Sécurité intérieure, de la Police grand-ducale, du Ministère de la Justice, du Parquet général, de la CNPD ainsi que de l'IGP.

2. Destinataires du projet :
   – Entreprises/Professions libérales : Oui ☒ Non ☐
   – Citoyens : Oui ☒ Non ☐
   – Administrations : Oui ☒ Non ☐

3. Le principe « Think small first » est-il respecté ? Oui ☐ Non ☐ N.a.[1] ☒
   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)
   Remarques/Observations :

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐
   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☒ Non ☐
   Remarques/Observations :

1 N.a. : non applicable.

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui ☐ Non ☒

   Remarques/Observations : n.a.

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☐ Non ☒

   Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☒ Non ☐ N.a. ☐

   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ? Retour d'informations automatisé dans le fichier central de la Police des suites réservées aux procès-verbaux en matière de police judiciaire par les autorités judiciaires.

   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? Oui ☒ Non ☐ N.a. ☐

   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ? Le projet concerne principalement la protection des données à caractère personnel dans les fichiers de la Police.

8. Le projet prévoit-il :
   - une autorisation tacite en cas de non réponse de l'administration ? Oui ☐ Non ☐ N.a. ☒
   - des délais de réponse à respecter par l'administration ? Oui ☐ Non ☐ N.a. ☒
   - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui ☐ Non ☐ N.a. ☒

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui ☐ Non ☐ N.a. ☒

   Si oui, laquelle :

10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui ☐ Non ☐ N.a. ☒

    Sinon, pourquoi ?

11. Le projet contribue-t-il en général à une :

    a) simplification administrative, et/ou à une Oui ☒ Non ☐

    b) amélioration de la qualité réglementaire ? Oui ☒ Non ☐

    Remarques/Observations :

---

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui ☒ Non ☐

Si oui, quel est le délai pour disposer du nouveau système ? 6 mai 2023, respectivement 6 mai 2026 au plus tard, lorsque cela exige des efforts disproportionnés.

14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui ☒ Non ☐ N.a. ☐

Si oui, lequel ?

Remarques/Observations :

Egalité des chances

15. Le projet est-il :
- principalement centré sur l'égalité des femmes et des hommes ? Oui ☐ Non ☒
- positif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒

  Si oui, expliquez de quelle manière :
- neutre en matière d'égalité des femmes et des hommes ? Oui ☒ Non ☐

  Si oui, expliquez pourquoi :
- négatif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒

  Si oui, expliquez de quelle manière :

16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui ☐ Non ☐ N.a. ☒

Si oui, expliquez de quelle manière :

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

---

5 Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

Impression: CTIE – Division Imprimés et Fournitures de bureau