

JUSTEL - Législation consolidée

http://www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=fr&la=F&nm=2021031874

Dossier numéro : 2021-08-04/01

Titre

4 AOÛT 2021. - Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique

Source : JUSTICE

Publication : Moniteur belge du 04-08-2021 page : 77908

Entrée en vigueur : 04-08-2021

Table des matières

Art. M

Texte

Article M.

A Mesdames et Messieurs les Bourgmestres,
Au Commissaire général de la police fédérale.

Pour information à :

Mesdames et Messieurs les Procureurs généraux,
Madame et Messieurs les Gouverneurs de province,

Monsieur le Ministre-Président de la Région de Bruxelles-Capitale,

Monsieur le Procureur fédéral et Mesdames et Messieurs les Magistrats du parquet fédéral,

Mesdames et Messieurs les Commissaires d'arrondissement,

Monsieur le Président de la Commission Permanente de la police locale,

Mesdames et Messieurs les Chefs de corps de la police locale,

Madame et Messieurs les Présidents de l'Organe de contrôle de l'information policière, du Comité permanent de contrôle des services de police et de l'Inspection générale de la police fédérale et de la police locale.

Madame le Bourgmestre,

Monsieur le Bourgmestre,

Monsieur le Commissaire général,

I. CADRE GENERAL

La présente directive met en oeuvre l'article 44/4, § 4 de la Loi sur la fonction de police (ci-après LFP).

Elle vise d'une part à mettre en perspective et expliquer les principes d'interconnexion des banques de données visées à l'article 44/2 LFP entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique ainsi que les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent.

Elle énonce d'autre part les modalités relatives à l'interconnexion des banques de données.

Ces modalités et règles constituent des instructions¹ au sens de l'article 23 de la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil vis à vis des membres du personnel agissant sous Notre autorité, ainsi que des sous-traitants et des personnes agissant

sous leur autorité.

L'interconnexion constitue d'une part une forme de traitement de l'information au sens de l'article 26. 2° de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après loi relative à la protection des données), qui permet de partager les données entre les personnes qui ont le besoin d'en connaître dans le cadre de leurs missions légales.

D'autre part, l'interconnexion permet également d'apporter une plus-value aux données initialement traitées en les corrélant et en les enrichissant.

Nous renvoyons également, à cet égard, à la notion de fonction de police guidée par l'information, ce concept servant de fil rouge dans l'ensemble des processus policiers: sans donnée de base donnant lieu à des informations travaillées, la police n'est pas en mesure d'assurer adéquatement la fonction de police de base, ni la fonction de police spécialisée.

En tant que moyen de partage et moyen de faire circuler les données travaillées entre les personnes qui ont le besoin d'en connaître, Nous confirmons que l'interconnexion de banques de données est également conforme à l'article 3 de la loi relative à la protection des données ainsi qu'à la recommandation de la commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 à l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution de la gestion de la lutte contre le radicalisme et la menace terroriste dont le troisième rapport intermédiaire recommande de créer une " banque-carrefour de la sécurité " (voir troisième rapport intermédiaire sur le volet " architecture de la sécurité ", Doc. Chambre, 2015-16, n° 1752/008). Sans que cette directive ne vise la création proprement dite d'une banque- carrefour, elle rencontre néanmoins l'idée que l'interconnexion de banques de données est la règle de la gestion de l'information opérationnelle policière.

A nouveau, en matière de gestion de l'information opérationnelle, la CEP a également rappelé la nécessité de se rapprocher le plus possible du concept de traitement en temps réel², ce qui permet l'interconnexion.

Concrètement, l'interconnexion est matérialisée par une ou plusieurs des actions suivantes :

1. la possibilité via une seule recherche de consulter des données qui, originellement, sont traitées dans différentes banques de données et qui sont dès lors dispersées.

Par exemple, grâce à un outil technique (par exemple un outil ou application de recherche et d'indexation de données) qui permet de rechercher une personne ou un véhicule dans plusieurs banques de données, un membre de la police peut directement savoir si cette entité est connue dans la banque de données nationale générale, est connue dans la banque de données d' Interpol ou dans la banque de données N.SIS (Schengen)³.

2. la possibilité de réaliser des corrélations de données qui, sont traitées originellement dans différentes banques de données, ou d'établir des liens entre ces données, à l'aide d'outils d'analyse ou d'applications d'analyse ou, le cas échéant, de listes ou d'extraits. Toutefois, il faut mettre en oeuvre des mesures techniques et organisationnelles appropriées⁴, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie pour les droits et libertés des personnes physiques. Lorsque des listes ou des extraits sont utilisés, ils doivent bien sûr être supprimés lorsque le besoin cesse d'exister.

Illustrons ce point : chaque enquêteur travaille dans un registre d'enquête séparé, ce qui ne permet pas a priori de réaliser des recoupements au sein de la police intégrée. Il est bien entendu utile, afin précisément de faire des corrélations entre différentes informations, de fournir des outils d'analyse afin de permettre à certaines personnes dotées d'un profil ad hoc, sous certaines autorisations et conditions, de savoir par exemple si les mêmes " modi operandi " ou caractéristiques se retrouvent dans différents dossiers, afin de pouvoir faire des liaisons entre plusieurs faits ou enquêtes et de pouvoir travailler sur les résultats qui ressortent de la corrélation.

3. la possibilité d'enrichir les données: lorsque des sources internes ou tierces de référence sont consultées directement et automatiquement à travers les applications policières, les données nécessaires et pertinentes pourront être automatiquement récupérées et insérées dans le processus de traitement. Par exemple, les données initialement traitées sont complétées par les données issues de la banque de données tierce.

A titre exemplatif, si le Registre national des personnes physiques (RRN) est automatiquement consulté lors de la rédaction d'un procès-verbal dans une banque de données de traitement de base (ISLP, FEEDIS), les données pertinentes du RRN pourront être récupérées dans le procès-verbal.

Dans le même ordre d'idée, la banque de donnée prévue pour le contrôle qui doit être effectué en matière de suivi des personnes qui, moyennant le respect de conditions, sont en liberté ou ont été mises en liberté, peut enrichir via un système automatisé la Banque de données Nationale Générale, ci-après dénommée "BNG", afin de permettre un contrôle par les services de police du respect des conditions de mise en liberté.

Enfin, l'interconnexion se fait avec des données provenant d'autres banques de données policières opérationnelles ou avec des banques de données auxquelles les services de police ont accès par ou en vertu de la loi, du décret ou de l'ordonnance.

L'interconnexion constitue dès lors une opération plus vaste que la simple consultation d'une seule banque de données.

II. NOTION D'INTERCONNEXION

L'interconnexion au sens de la présente directive doit être comprise comme le traitement

i. via lequel plusieurs banques de données visées au point V sont simultanément et automatiquement consultées ou

ii. par lequel des informations et données à caractère personnel issues de banques de données visées au point V sont corrélées via une procédure automatisée ou

iii. par lequel des informations et données à caractère personnel issues de banques de données visées au point V sont enrichies via une procédure automatisée.

III. MODALITES DES INTERCONNEXIONS

L'interconnexion s'effectue conformément au cadre légal applicable en matière de gestion de l'information policière opérationnelle, dont les articles 44/1 et suivants de la LFP, le titre II de la loi relative à la protection des données et, en matière judiciaire, le code d'instruction criminelle.

En outre, l'interconnexion de banques de données par les services de police s'inscrit toujours dans le cadre de l'exercice de leurs missions policières opérationnelles, visées aux articles 14 et 15 LFP.

Nous rappelons également qu'à l'instar de toutes les données traitées dans le cadre des missions opérationnelles, les données partagées via un mécanisme d'interconnexion doivent, selon le prescrit de la LFP (articles 5/2, 17, 40, 44/1, §§ 3 et 4), faire l'objet d'un rapport aux autorités administratives et/ou judiciaires.

Au niveau de la mise en oeuvre de l'interconnexion, les modalités suivantes sont applicables :

1. il faut veiller, en fonction du processus de travail, à ce que, d'une part, seules les données pertinentes dans le cadre des missions policières opérationnelles de police administrative et de police judiciaire y figurent et, d'autre part, que soient d'office exclues les données qui ne peuvent être partagées sans profil spécifique justifiant le besoin d'en connaître. Par exemple les dossiers qui font l'objet d'une mesure visée à l'article 44/8 LFP.

Cette modalité permet d'assurer que seules les données adéquates, pertinentes et non excessives par rapport aux processus de travail sont partagées.

2. l'état de validation des informations accessibles via le mécanisme d'interconnexion et émanant entre autres des banques de données de base ou particulières doit être clairement indiqué (article 44/4, § 5, 5° LFP).

3. la catégorie de personnes concernées dont relève la personne enregistrée dans les banques de données policières opérationnelles doit être identifiable de manière non ambiguë. Il est essentiel qu'une distinction claire soit opérée, notamment entre les suspects et les victimes ou témoins.

4. en principe, une consultation préalable ou simultanée de la BNG, qui constitue la source de référence pour les mesures à prendre par les services de police visées à l'article 44/7, al. 1, 5° LFP ou d'autres banques de données de référence, est nécessaire le cas échéant, à moins que cela ne soit excessif pour une recherche ponctuelle.

En outre, la BNG doit toujours être alimentée conformément à l'article 44/7 LFP dernier alinéa, le cas échéant, via l'indication des mesures à prendre soit sur la base d'une décision des autorités compétentes de police administrative ou de police judiciaire, soit en fonction de l'existence des antécédents de police administrative ou de police judiciaire.

5. l'obligation de respecter les règles et conditions d'accès et les délais de conservation respectifs pour les banques de données interconnectées. Cette modalité traduit donc le fait que l'interconnexion ne permet bien entendu pas de contourner les règles d'accès et les durées de conservation. Si par exemple un membre des services de police n'a pas accès aux informations non concrètes, il ne pourra pas, via le mécanisme d'interconnexion, accéder à ce type de données.

6. la ou les banques de données utilisées lors de l'interconnexion et le service responsable de l'information doivent être identifiables.

Il s'agit d'assurer la transparence quant aux sources d'informations traitées.

7. l'obligation pour les responsables des traitements d'enregistrer dans le registre des traitements de la police (le RegPol)⁵, les banques de données qui sont corrélées ou interconnectées pour les traitements dont ils sont responsables ;

8. l'obligation pour les services de police de mettre à jour conformément à l'article 44/5, § 6 les données, lorsqu'il appert qu'elles ne sont plus exactes ou ne remplissent plus les conditions pour pouvoir être traitées ;

9. une interconnexion ne peut être réalisée qu'avec une banque de données disposant de fichiers de journalisation, conformément à l'article 44/4, § 2 LFP. En effet, cet article ainsi que l'article 56 de la loi relative à la protection des données imposent, notamment au responsable de traitement, d'établir des fichiers de journalisation (" logging ") pour tous les systèmes de traitement opérationnels automatisés.

10. les outils d'analyse et les applications d'analyse utilisés pour faire des corrélations doivent pouvoir être audités en vue d'expliquer leur fonctionnement et à tout le moins des explications doivent pouvoir être fournies sur :

- i. les catégories de banques de données et de données qui seront utilisées en fonction du processus de travail ;
- ii. les raisons pour lesquelles ces catégories sont jugées pertinentes ;
- iii. le type de résultats auxquels les corrélations peuvent aboutir et la manière dont ils sont traités dans les processus policiers ;
- iv. les mécanismes mis en place pour respecter les principes de protection des données.

Cet audit se basera également sur l'analyse d'impact réalisée conformément à l'article 58 de la loi relative à la protection des données du 30 juillet 2018 préalablement à l'utilisation des outils ou applications d'analyse .

Chaque service de police doit, en outre, à tout moment, être capable d'identifier qui a consulté quoi, quand et pour quelle raison. Il doit également opérer des vérifications de la licéité du traitement et réaliser des autocontrôles.

Conformément aux obligations légales et réglementaires ainsi qu'aux injonctions de l'Organe de contrôle, chaque service de police procèdera à la mise en place d'une politique proactive basée sur un système de contrôle a posteriori sur les consultations effectuées afin d'en vérifier la légitimité et la légalité.

Cette politique de contrôle tient compte des principes et de la philosophie repris dans la directive relative à la motivation des consultations des banques de données.

Cette politique prévoira, entre autres, des contrôles systématiques et proactifs sur l'utilisation et/ou les consultations des banques de données policières. Dans ce cadre, il sera notamment procédé de manière périodique à des contrôles par échantillons (de manière aléatoire) via des loggings (analyse des motivations et des journaux de consultations).

IV. REGLES D'ACCES DES MEMBRES DES SERVICES DE POLICE

Si, comme Nous l'avons déjà mentionné, l'interconnexion des banques de données vise avant tout à permettre