Juin
2021

La radicalisation au prisme des banques de données

Addendum
Note complémentaire relative aux directives sur la gestion de l'information policière

Isabelle Detry
Benjamin Mine
Patrick Jeuniaux

Nationaal Instituut voor Criminalistiek en Criminologie
Institut National de Criminalistique et de Criminologie

Folks, Authorities and Radicalism : between polarization and social construction (FAR).

Projet financé par la Politique scientifique fédérale (**BELSPO**) – Contrat **#BR/175/A4/FAR**.

ADDENDUM

Note complémentaire relative aux directives sur la gestion de l'information policière

1. Contextualisation

Depuis la finalisation du rapport sur « la radicalisation au prisme des banques de données »[1], plusieurs directives communes des ministres de la Justice et de l'Intérieur sont venues préciser les règles de gestion de l'information policière dont parle ce rapport. Toutes ces directives ont un caractère contraignant, aussi nous semblait-il important de publier la présente note, qui vient mettre à jour le rapport avec des éléments importants.

Étant donné le caractère technique de la matière et la brieveté de cette note, le lecteur est invité à prendre connaissance du rapport qui introduit les notions nécessaires à sa compréhension.

2. Trois directives

Les directives concernées sont actuellement au nombre de trois et ont été publiées au Moniteur belge le 28 janvier 2021, le 2 février 2021 et le 28 mai 2021.

2.1 La première directive

Celle du **28 janvier 2021** détermine des mesures adéquates, pertinentes et non excessives relatives à **l'interconnexion ou la corrélation** des banques de données techniques suite à l'utilisation de caméras ou de systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, visées à l'article 44/2, § 3 de la loi sur la fonction de police (LFP), avec les banques de données visées à l'article 44/2, §§ 1er et 2 LFP, 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.

2.2 La deuxième directive

Celle du **2 février 2021** détermine les **modalités de communication des données** à caractère personnel et informations traitées dans le cadre de leurs missions de police administrative et judiciaire, telles que visées aux articles 14 et 15 de la LFP, par les services de police et à l'accès direct et l'interrogation directe de la Banque de données Nationale Générale.

2.3 La troisième directive

La directive du 28 mai 2021 concerne les règles d'accès des membres des services de police à la Banque de Données Nationale générale, aux banques de données de base, particulières et techniques.

Cependant, un erratum a été publié trois jours après, disant que « […] le texte publié sous le numéro 2021/30853, à la page 55280, doit être considéré comme inexistant. Le texte sera republié séparément. ». À notre connaissance, ce texte n'a à ce jour pas encore été republié au Moniteur belge.

[1] Isabelle Detry, Benjamin Mine, & Patrick Jeuniaux (2021). La radicalisation au prisme des banques de données, Rapport de recherche, Institut National de Criminalistique et de Criminologie, Direction Opérationnelle de Criminologie, Collection des rapports et notes de recherche. 65 p. https://incc.fgov.be/la-radicalisation-au-prisme-des-banques-de-donnees

Enfin, un rappel des règles relatives à la communication des données à caractère personnel et informations aux services de police étrangers, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux devrait être également publié prochainement.

3. Commentaire sur la deuxième directive

Nous décrivons à présent le contenu de la directive relative aux modalités de communication des données à caractère personnel et informations du 2 février 2021 en ce qu'elle complète et précise le contenu du rapport précité en son point 1.1.6 « Les accès aux données et informations contenues dans la BNG ».

Cette directive contraignante vise à encadrer l'ensemble des possibilités de communication par les services de police à des tiers (nationaux) des données à caractère personnel et informations enregistrées dans la BNG. La lecture de cette directive laisse à penser que les services de police entendent se prémunir contre une demande croissante de communication de leurs données et éviter d'être tenus pour responsables, en tant que producteur de données, des atteintes à la vie privée que leur communication pourraient générer. En effet, si, de manière générale, les services de police se réservent le droit de communiquer une donnée ou une information lorsqu'ils l'estiment nécessaire pour l'accomplissement des missions légales du destinataire, et ce en l'absence de toute demande posée, la directive encadre par contre très clairement le devoir ou la possibilité des services de police de communiquer, une donnée à un tiers à la demande de celui-ci. Il est ainsi recommandé au service de police auquel la demande est adressée de toujours soumettre cette demande à sa hiérarchie et, en tout état de cause, de vérifier la réalité du droit du demandeur d'obtenir cette information. Ainsi, même si le demandeur est l'Organe de Coordination pour l'Analyse de la Menace (OCAM), un service de renseignement, la Cellule de Traitement des Informations Financières (CTIF), l'Office des Etrangers (OE) ou le service de recherche des douanes, il est enjoint au service de police de contrôler que l'identité du demandeur est bien celle d'un de ces services et que « le traitement ultérieur par ledit service est légalement autorisé et que l'obtention de ces données par le service tiers repose sur un besoin actuel de partage ». Au surplus, si la donnée concerne un suspect ou une affaire au stade de l'information au parquet, l'accord préalable du parquet doit être demandé ; si on en est au stade de l'instruction, il faudra au cas par cas demander l'accord du parquet.

La directive affirme par ailleurs très clairement qu'il ne peut y avoir d'autorisation générale préalable du parquet en la matière, fut-ce dans le domaine de la lutte contre le terrorisme et l'extrémisme violent.

De même, la directive rappelle que les codes d'utilisation des RIR doivent être respectés ; et le statut de la personne dans la BNG doit être précisé (suspect, auteur, témoin, victime).

Le service de police doit également vérifier que le destinataire est bien soumis à une obligation de confidentialité.

Pour terminer, la directive rappelle l'obligation pour le service de police d'évaluer, avant toute communication, la qualité des données. Si la validation n'a pas été (ou pas pu être) effectuée, et qu'il n'y a donc pas encore d'enregistrement dans la BNG, il convient de le mentionner au destinataire.

Lorsque le demandeur est une autorité publique belge, un organe ou un organisme public ou d'intérêt public faisant partie de la « liste », le service de police doit procéder à une triple vérification :

(1) la donnée demandée est-elle une donnée à caractère personnel ?
(2) si oui, le demandeur figure-t-il dans la liste ?
(3) si oui, le destinataire démontre-t-il que les données demandées sont adéquates, pertinentes et non excessives par rapport aux besoins pour lesquels il souhaite les obtenir ?

En cas de réponse négative aux questions (2) et (3), la donnée ne pourra être transmise.

Si la demande concerne une communication récurrente et volumineuse, il faudra alors, préalablement à la transmission, la conclusion d'un protocole d'accord entre le destinataire et le responsable du traitement qui détermine (1) les catégories de membres du personnel autorisées, (2) les mesures de sécurité en relation avec cette communication (la voie électronique doit être privilégiée), (3) les conditions spécifiques, à savoir les interdictions de traitement ultérieur et d'utilisation à d'autres fins et la limitation du droit à l'information de la personne concernée en l'absence d'autorisation préalable.

Pour terminer, la directive aborde également la question des conditions auxquelles doivent répondre les demandes d'obtention d'un droit d'accès direct ou d'un droit d'interrogation directe, de même qu'une demande de faire partie de la « liste » des autorités, organes, organismes autorisés pour l'exercice de leurs missions à obtenir la communication de certaines données.

Ainsi, en ce qui concerne la demande d'accès direct et d'interrogation directe, il est rappelé que ce droit ne peut être accordé que par arrêté royal et après avis de l'Organe de contrôle de l'information policière (COC) et qu'il ne le sera que si cette demande est légale et proportionnelle. Pour vérifier le respect de ces conditions, toute demande devra, au minimum, être accompagnée des informations suivantes : (1) les finalités du traitement, (2) l'identification du service demandeur comme appartenant à la chaine pénale, (3) le contexte de la demande et (4) la motivation opérationnelle de la demande. Au surplus, la directive précise que les modalités concrètes fonctionnelles et techniques seront intégrées dans un protocole d'accord entre le demandeur et la Direction de l'information policière et des moyens ICT de la Police de fédérale (DRI).

L'adjonction d'une entité dans la liste des autorités, organes ou organismes autorisés requiert, quant à elle, également différentes vérifications et une procédure particulière. La liste est arrêtée par les ministres de la Justice et de l'Intérieur sur la base d'une proposition du Comité information et ICT. Les avis préalables du COC et du Collège des Procureurs Généraux sont sollicités. Il est précisé que l'avis du COC n'est pas contraignant.

*
* *