Initiative parlementaire 17.423 : Obligation de collaborer à la procédure d'asile. Possibilité de contrôler les téléphones mobiles. Avant-projet et rapport explicatif de la Commission des institutions politiques du Conseil national du 14 février 2020

Procédure de consultation : avis de l'Organisation suisse d'aide aux réfugiés

Berne, le 27 mai 2020

Table des matières

1 Introduction

L'Organisation suisse d'aide aux réfugiés (OSAR) est reconnaissante de pouvoir prendre position sur l'avant-projet susmentionné et expose dans le présent document son avis sur les aspects qu'elle juge les plus importants. L'absence de commentaire de l'OSAR sur quelque aspect que ce soit ne doit pas être interprété comme une approbation.

L'OSAR rejette la proposition de la Commission des institutions politiques du Conseil national (CIP-N) visant à modifier la loi sur l'asile et la loi sur les étrangers et l'intégration afin de compléter l'obligation de collaborer et la possibilité de contrôler les supports de données mobiles. Celle-ci constitue une atteinte grave au respect de la vie privée, l'un des droits fondamentaux. L'OSAR est d'avis que les conditions pour une telle atteinte à un des droits fondamentaux ne sont pas remplies (art. 36 Cst. : base légale, intérêt public, proportionnalité, protection de l'essence du droit fondamental).

Pour justifier l'introduction d'une base légale en Suisse, le CIP-N souligne que d'autres États européens ont eux aussi introduit des réglementations correspondantes[1]. Toutefois, dans son rapport explicatif, elle ne présente que de manière brève et de surcroit unilatérale la pratique en vigueur dans les pays concernés. Elle ne fait ainsi aucune mention des discussions controversées, des problèmes soulevés et de l'application extrêmement limitée des réglementations introduites ces dernières années. Ainsi, les observations de la mise en œuvre de ces réglementations en Allemagne et dans d'autres pays européens ne sont pas évoquées, alors qu'elles montrent à quel point la question est complexe. Ces observations illustrent les nombreuses questions et problèmes non résolus concernant divers principes fondamentaux : état de droit, droit fondamental au respect de la vie privée, proportionnalité et protection des données. En outre, elles montrent, notamment en Allemagne, que ces mesures génèrent des coûts très élevés et que dans de rares cas seulement il est possible de tirer réellement parti des investigations menées[2]. Il est donc erroné de parler de « méthode efficace », comme le prétend la CIP-N dans son rapport explicatif[3]. Selon l'OSAR, les observations menées dans d'autres pays ne justifient aucunement le point de vue optimiste exprimé par la CIP-N. Au contraire, elles constituent davantage un avertissement quant aux risques qu'entraînerait l'introduction de mesures aussi extrêmes.

L'OSAR estime qu'aucune base légale en la matière ne devrait être introduite, car elle ne serait compatible ni avec les garanties de l'État de droit et ni avec les droits fondamentaux. Il apparaît qu'aucune évaluation suffisante des risques et des effets d'une telle base légale n'a été effectuée. Pourtant, compte tenu des atteintes graves aux droits fondamentaux qu'elle constituerait, des clarifications et explications détaillées seraient nécessaires, afin d'apporter une démonstration convaincante de la prise en compte des différents problèmes et questions

1 17.423 Initiative parlementaire, obligation de collaborer à la procédure d'asile. Possibilité de contrôler les téléphones mobiles, avant-projet et rapport explicatif de la Commission des institutions politiques du Conseil national du 14 février 2020 (CIP-N, rapport explicatif), paragraphe 1.3.

2 Voir le point 5.1 ci-dessous, qui se fonde notamment sur : Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf. L'étude contient des informations détaillées sur la situation juridique et la pratique en Allemagne ainsi qu'un bref aperçu de la situation juridique et de la pratique au Danemark, en Norvège, en Belgique, en Autriche et au Royaume-Uni.

3 CIP-N, Rapport explicatif, point 1.2.

soulevés concernant l'État de droit, le droit fondamental au respect de la vie privée, la proportionnalité et la protection des données. Or, ces explications sont totalement absentes du projet de consultation.

2 L'essentiel en bref

L'OSAR rejette la proposition de la CIP-N de modifier la loi sur l'asile et la loi sur les étrangers et l'intégration afin de compléter l'obligation de collaborer et la possibilité de contrôler les supports de données mobiles. La mesure constitue une atteinte grave au droit au respect de la vie privée (art. 13 Cst., art. 8, al. 1 CEDH) et les conditions susceptibles de justifier une telle atteinte ne sont pas remplies :

- Une **base légale** insuffisante : les restrictions graves aux droits fondamentaux doivent reposer sur une loi au sens formel (art. 36, al. 1 Cst). Or, l'avant-projet prévoit que les aspects centraux soient réglés par ordonnance (tri des données pertinentes pour l'établissement de l'identité, définition des données collectées, réglementation quant à l'accès). En outre, la base n'est pas suffisamment définie, car elle comprend de potentiels futurs supports de données amenés à apparaître en fonction des développements technologiques.
- **Proportionnalité** : l'OSAR considère que l'obligation imposée aux personnes requérantes d'asile de remettre leurs supports de données mobiles aux fins d'établissement de leur identité et le droit correspondant du Secrétariat d'Etat aux migrations (SEM) de contrôler ces supports sont disproportionnés.
    - La mesure n'est pas nécessaire, car la finalité n'exige pas des mesures portant une telle atteinte aux droits fondamentaux. En outre, l'avant-projet ne respecte pas le principe d'*ultima ratio*.
    - L'avantage limité est disproportionné par rapport à la gravité de l'atteinte au respect de la vie privée.
    - Compte tenu des conséquences procédurales graves prévues en cas de violation de l'obligation de collaborer, on ne peut parler de remise volontaire des supports de données.
- Il manque un **contrôle par un tribunal** de la légalité et de la proportionnalité, qui constitue pourtant une exigence impérative dans les procédures pénales concernant les personnes soupçonnées d'infractions graves. Les procédures d'asile ne concernent pas des criminels potentiels, mais des personnes cherchant protection. Il est d'autant plus choquant qu'elles ne bénéficient pas de ces mêmes garanties procédurales.
- **Protection des données** : la procédure d'asile implique le traitement de données sensibles. Il s'agit, à toutes les étapes de la procédure, de garantir la protection des données des personnes concernées ainsi que le principe de proportionnalité. Seules des réglementations qui ont été examinées, évaluées et approuvées par le Préposé fédéral à la protection des données et à la transparence (PFPDT) doivent être introduites. Dans les autres pays européens, lors des débats sur l'introduction de réglementations similaires, des problèmes importants ont été relevés par diverses parties en ce qui concerne la législation sur la protection des données.
- **Coûts** : la mesure proposée entraîne des coûts très élevés totalement disproportionnés par rapport au faible profit qui peut en être tiré.
- La proposition dépasse la finalité visée de l'initiative parlementaire, car elle étend cette finalité à l'établissement de l'itinéraire parcouru par la personne requérante et étend l'obligation de collaborer à la procédure d'exécution du renvoi.

3 Base légale

La modification de la loi prévue constitue une atteinte à la protection de la vie privée (art. 13 Cst., art. 8, al. 1 CEDH), plus précisément au droit à l'autodétermination informationnelle. La CIP-N le confirme d'ailleurs elle-même dans son rapport explicatif, concédant que la protection de la vie privée est un « droit fondamental important, qui doit bien entendu aussi être accordé dans la procédure d'asile »[4]. L'OSAR est d'avis que la consultation des supports de données mobiles dans les procédures d'asile représente une **atteinte grave à la vie privée.** Les téléphones portables des personnes requérantes d'asile stockent un grand nombre de données personnelles et parfois très sensibles. En outre, une consultation des supports par les autorités concernerait également des tiers non impliqués. En effet, les autorités auraient alors accès, par exemple, aux données des membres de la famille et des proches ayant soutenu la personne requérante ou à la correspondance de la personne requérante avec les avocat-e-s ou les médecins, sans que ces tiers n'aient donné leur consentement personnel préalable. Selon le rapport explicatif, les données personnelles de tiers ne peuvent être exploitées[5]. Toutefois, compte tenu de l'abondance des données à consulter, dont la correspondance, cette délimitation semble se heurter à des difficultés pratiques. Le rapport explicatif n'apporte aucune explication sur les moyens de garantir cette délimitation.

Le SEM a également décrit la mesure comme une atteinte grave au droit fondamental à l'autodétermination informationnelle dans une réponse aux médias qui a eu lieu à la suite de l'évaluation du projet pilote en 2019[6]. La Société pour les libertés civiles (*Gesellschaft für Freiheitsrechte*) en Allemagne a elle aussi souligné dans son étude sur la pratique en vigueur en Allemagne : « La consultation des smartphones, qui contiennent une grande quantité de données sensibles provenant des domaines les plus divers de la vie, représente sans aucun doute une atteinte grave aux droits fondamentaux. »[7]

Selon la Constitution (art. 36, al. 1), une atteinte grave au droit à la vie privée nécessite **au sens formel une loi.** De l'avis de l'OSAR, le projet de loi ne répond pas à ces exigences. Il est certes prévu que les points fondamentaux – l'obligation de remettre les supports de données et le droit du SEM de consulter ces données – fassent l'objet d'une réglementation dans la loi sur l'asile. Toutefois, il est également prévu de fixer plusieurs aspects centraux uniquement par ordonnance (modalités de tri des données pertinentes pour l'établissement de l'identité, définition des données à collecter, réglementation concernant l'accès, nouv. art. 8a al. 5 LAsi). Les explications fournies dans le rapport explicatif sont également trop vagues en ce qui concerne le type de données exact qui devra être collecté. En outre, le projet ne fournit pas assez d'informations claires et de directives concrètes sur la procédure prévue pour la

4 CIP-N, Rappport explicatif, point 2.1.
5 CIP-N, Rapport explicatif, section 3.1, art. 8a al. 3 à 5.
6 Der Bund, Handys von Asylsuchenden geprüft – und fündig geworden, 09.08.2019, https://www.derbund.ch/schweiz/standard/bund-kontrolliert-handys-von-asylsuchenden/story/29531805.
7 Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 9.

sélection des données, sur leur stockage intermédiaire ni sur leur consultation. L'OSAR est d'avis que ces aspects devraient être inclus dans la loi elle-même[8].

La base légale doit également être suffisamment définie. Le rapport explicatif suggère que la liste des supports de données proposée dans l'avant-projet (nouv. art. 8a, al. 2, LAsi) ne soit pas exhaustive afin qu'elle puisse prendre en compte les développements techniques futurs. L'étendue des développements techniques futurs étant totalement inconnue, cette disposition apparaît bien **trop vague** pour constituer une base légale qui autorise une atteinte aussi importante à la vie privée. À cet égard également, les conditions nécessaires à une base légale ne sont pas remplies.

4 L'intérêt public

4.1 Etablissement de l'identité, de la nationalité et de l'itinéraire

Selon le rapport explicatif, le projet de loi poursuit une finalité d'intérêt public, à savoir l'établissement de l'identité des personnes requérantes d'asile, de leur nationalité et de leur itinéraire. Toutefois, l'OSAR rappelle que la finalité d'établir l'itinéraire ne figurait pas dans l'initiative parlementaire 17.423, qui constitue la base de ce projet de loi. L'initiative parlementaire demandait la consultation des supports de données avec pour seule finalité de clarifier l'*identité* de la personne requérante d'asile. **Or, l'établissement de l'itinéraire poursuit une finalité complètement différente**. Aux yeux de l'OSAR, l'extension ultérieure de la finalité est d'autant plus discutable qu'elle implique la consultation de données plus étendues, qui ne seraient d'aucune utilité à la poursuite de la finalité initiale (établissement de l'identité).

En **Allemagne,** la réglementation **évoque uniquement l'établissement de l'identité et de la nationalité**[9], et non de l'itinéraire. Lors de son introduction, Pro Asyl a toutefois exprimé ses craintes quant à une extension à l'établissement de l'itinéraire dans la pratique et a souligné les différences entre ces deux finalités : « L'examen de l'itinéraire et l'établissement de l'identité poursuivent cependant deux finalités complètement différentes. Il est ici particulièrement évident que le principe de finalité ne sera pas respecté. Il est à craindre que, dans la pratique, l'Office fédéral utilise les données des personnes concernées dans une autre finalité. En particulier, il est à supposer que les données seront utilisées pour retracer l'itinéraire [de la personne requérante], afin d'identifier un État membre responsable [de la demande d'asile] en vertu du règlement Dublin III et de renvoyer la personne requérante dans cet État membre. »[10] Concernant l'introduction d'un tel règlement en Suisse, il est là aussi à supposer que l'établissement de l'itinéraire a été ajouté avec pour finalité principale de déterminer l'État membre Dublin responsable. En effet, l'évaluation des supports de données pourrait éventuellement permettre de déterminer dans quel Etat Dublin la personne requérante est entrée

8 Pour des raisons de protection des données également, les éléments fondamentaux devraient être fixés au sens formel par une loi, voir le point 8 ci-dessous.

9 §15 al. 2 n° 6 et §15a loi allemande sur l'asile.

10 Prise de position de PRO ASYL du 27 mars 2017 devant la commission des affaires intérieures du Bundestag allemand concernant le projet de loi du gouvernement fédéral : Projet de loi pour une meilleure application de l'obligation de quitter le pays, BR-Drucksache 179/17, 22.03.2017, https://www.bundestag.de/resource/blob/500016/c93c5454d698d8b0e8f08117cefae473/18-4-825-A-data.pdf, p. 20.

en premier. Toutefois, le règlement Dublin III énumère déjà de nombreuses possibilités (preuves et indices) qui peuvent être utilisées pour déterminer l'État responsable. Par conséquent, une évaluation des supports de données n'est pas nécessaire pour déterminer la responsabilité et n'apparaît pas justifiée, compte tenu de la gravité de l'atteinte au droit fondamental.

4.2 Passeurs et crimes de guerre

Le rapport explicatif indique en second lieu que la consultation des supports de données électroniques peut également contribuer à lutter contre les activités des passeurs et à élucider les crimes de guerre. Il convient toutefois de se demander si les modifications proposées pourront réellement contribuer à la lutte contre les activités de passeurs et à l'élucidation des crimes de guerre. Ce n'est probablement que dans des cas exceptionnels et isolés que le SEM examinera de telles informations[11]. Ces objectifs ne sont d'ailleurs mentionnés que superficiellement dans le rapport explicatif. Or, cette seule mention ne suffit pas à justifier l'atteinte grave aux droits fondamentaux qui est prévue. En outre, il importe de ne pas considérer de manière générale les personnes cherchant protection comme des criminels de guerre ou des passeurs potentiels.

5 Proportionnalité

Toute mesure qui porte atteinte à un droit fondamental doit être adéquate et nécessaire (*ultima ratio*, aucune mesure plus légère envisageable). En outre, la finalité et l'effet de cette atteinte à un droit fondamental doivent être proportionnels (proportionnalité au sens étroit). L'OSAR est d'avis que ces conditions ne sont pas remplies en ce qui concerne l'obligation imposée aux personnes requérantes d'asile de remettre leurs supports de données électroniques et en ce qui concerne le droit du SEM de les contrôler.

5.1 Mesure inadéquate et inutile

Dans le cadre du projet pilote mené de novembre 2017 à mai 2018 dans les centres fédéraux pour requérants d'asile de Chiasso et Vallorbe, les personnes requérantes d'asile avaient la possibilité de soumettre leurs supports de données mobiles. Selon des investigations menées par des médias, dans seulement 11 % des cas (sur un total de 565 supports de données ayant été consultés), des « indices utiles » concernant l'identité et l'origine ont pu être trouvés[12]. Compte tenu de l'ampleur du projet pilote et de l'intérêt public marqué, il est surprenant

[11] Dans le cadre du projet pilote mené de novembre 2017 à mai 2018 dans les centres fédéraux pour requérants d'asle de Chiasso et de Vallorbe (sur une base volontaire), des informations ont été transmises aux autorités de police et de sécurité dans 5 cas sur 565 pour des soupçons d'infractions pénales : Der Bund, Handys von Asylsuchenden geprüft – und fündig geworden, 09.08.2019, https://www.der-bund.ch/schweiz/standard/bund-kontrolliert-handys-von-asylsuchenden/story/29531805.

[12] Der Bund, Handys von Asylsuchenden geprüft – und fündig geworden, 09.08.2019, https://www.der-bund.ch/schweiz/standard/bund-kontrolliert-handys-von-asylsuchenden/story/29531805. Dans le cadre du projet pilote déjà, des données sur l'itinéraire de voyage ont été systématiquement collectées, bien que cette finalité supplémentaire n'était même pas prévue par l'initiative parlementaire 17.423 (voir ci-dessus chapitre 4.1). Selon le SEM, des « informations utiles » ont été trouvées dans 4 % des cas.

que le SEM n'ait publié ni le rapport final ni les résultats concrets du projet et que les médias aient été les seuls à diffuser l'information. Le rapport explicatif de la CIP-N n'offre pas non plus la transparence nécessaire. Il ne contient que des informations très générales sur le projet pilote et aucune information quantitative sur le nombre de cas ayant permis de trouver des informations utiles. En particulier, il n'indique pas quels types d'informations se fondent concrètement sur quels types de données, comment leur utilité est évaluée, quelles conséquences ces informations ont eues et dans combien de cas (confirmation ou infirmation des informations fournies par les personnes requérantes d'asile). Le rapport explicatif n'indique pas non plus si ces informations n'auraient pas pu être obtenues par le biais d'autres mesures plus légères. En bref, l'utilité de consulter les données ne peut être vérifiée en raison d'un manque de transparence et elle n'est pas attestée de manière crédible.

L'expérience de l'Allemagne corrobore les doutes concernant l'utilité avancée par le projet : dans son étude de décembre 2019, la Société pour les libertés civiles (*Gesellschaft für Freiheitsrechte*), se fondant sur des réponses du gouvernement allemand à des questions de parlementaires, indique que : « Dans environ un quart des cas, la consultation des supports de données apparaît défaillante pour des raisons techniques. De janvier 2018 à juin 2019, un total d'environ 17 000 supports de données ont été consultés avec succès. Depuis le début de l'évaluation des supports de données, moins de la moitié d'entre eux en moyenne se sont révélés utilisables et l'évaluation des informations récoltées n'a abouti que dans un à deux pour cent des cas à une infirmation des déclarations fournies par les personnes requérantes. Dans tous les autres cas, le test a confirmé les déclarations des personnes requérantes d'asile. »[13]

En outre, le gouvernement allemand a admis lui-même que l'utilité escomptée ne pouvait tout simplement pas être prouvée de manière empirique : « Étant donné que, outre la consultation des supports de données, de nombreux autres aspects entrent en ligne de compte dans l'évaluation globale, il n'est pas possible de déterminer statistiquement dans quelle mesure l'évaluation des supports de données des personnes requérantes d'asile par le BAMF [Office fédéral allemand des migrations et des réfugiés] a jusqu'à présent conduit ou contribué de manière significative à réfuter ou à confirmer les déclarations des personnes requérantes d'asile quant à leur origine/identité/nationalité. Même si les données sélectionnées contredisent l'origine alléguée, il arrive, dans certains cas, que d'autres constatations conduisent finalement à la confirmation de cette origine ».[14]

Selon la Société pour les libertés civiles (*Gesellschaft für Freiheitsrechte*), l'évaluation automatique des données, y compris l'analyse des langues et des dialectes à partir des messages vocaux ou des conversations de type chats, induit également un grand potentiel d'erreur, qui peut entraîner une discrimination à l'égard des personnes requérantes d'asile de certains pays d'origine. En raison d'un manque de données sur la fiabilité de la reconnaissance vocale, les autorités et les tribunaux ne sont pas en mesure d'évaluer correctement la valeur probante

[13] Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 5.

[14] Réponse du gouvernement fédéral à la question parlementaire des députés Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, d'autres députés et du groupe parlementaire DIE LINKE, Drucksache 19/2186, Ergänzende Informationen zur Asylstatistik für das erste Quartal des Jahres 2018, Drucksache 19/3148, 03.07.2018, par. 8, p. 26, https://dip21.bundestag.de/dip21/btd/19/031/1903148.pdf.

de l'évaluation automatique, ce qui est problématique du point de vue de l'État de droit[15]. Dans le projet de consultation, la méthode d'évaluation reste floue. Une chose est sûre : si l'évaluation proposée par l'avant-projet devait être assurée par des mécanismes automatiques, ceux-ci soulèveraient en Suisse les mêmes préoccupations concernant l'Etat de droit. Si, en revanche, l'évaluation devait être effectuée uniquement manuellement par le personnel du SEM, cela induirait un investissement énorme en temps et en travail et entraînerait donc une augmentation des coûts.

Au vu de ces observations empiriques, on peut douter que l'obligation de remettre ces supports de données électroniques et l'évaluation de ceux-ci soient adaptées à la finalité visée. Du point de vue de l'OSAR, le faible bénéfice attendu ne saurait en aucun cas justifier l'atteinte grave à la vie privée qui en résulterait, raison pour laquelle la mesure est disproportionnée.

5.2 Nécessité et rapport entre la finalité et l'effet

Pour qu'une mesure portant atteinte à un droit fondamental soit proportionnée, elle doit être nécessaire. Pour ce faire, sa finalité ne doit pas pouvoir être atteinte par le biais de mesures moins incisives, qui constitueraient une restriction moins forte à ce droit fondamental. Selon l'OSAR, ce principe n'est pas observé dans le projet de la CIP-N : la formulation du nouv. art. 8, al. 1, let. g LAsi du projet de loi (« si son identité, sa nationalité ou son itinéraire ne peuvent pas être établis sur la base de documents d'identité, ni par d'autres moyens raisonnables ») est trop vague. Il n'est pas précisé qu'une telle mesure n'intervient qu'en dernier recours (*ultima ratio*), à savoir uniquement si l'identité, la nationalité ou l'itinéraire **ne peuvent pas être établis au moyen d'une mesure portant une atteinte moindre à la vie privée.** Cette exigence centrale est également absente du rapport explicatif. Le rapport explicatif souligne que « les intéressés doivent dans tous les cas avoir d'abord la possibilité de donner d'eux-mêmes des indications sur leur nationalité, leur identité ou leur itinéraire »[16], garantie qui est une évidence. En outre, le rapport poursuit : « En vertu du principe de proportionnalité, on commencera toujours par établir l'identité « par d'autres moyens », dès lors que cette manière de faire implique une charge de travail moindre qu'une analyse de données électroniques. »[17] En outre, le rapport explicatif concède qu'une « expertise LINGUA ne doit pas être envisagée [...] avant l'analyse de données électroniques, car cette procédure requiert beaucoup de temps et de préparatifs. »[18] L'OSAR est d'avis que cette argumentation est caduque en ce sens que le facteur décisif pour évaluer la proportionnalité de l'*atteinte à un droit fondamental* n'est pas la charge de travail (assumée en premier lieu par l'État), mais l'*étendue de l'atteinte à un droit fondamental*. La loi allemande sur l'asile contient d'ailleurs cette condition préalable : l'évaluation d'un support de données n'est autorisée que si elle est nécessaire pour établir l'identité et la nationalité et que la finalité de la mesure ne peut être atteinte par des moyens plus légers[19].

---

15 Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 20.

16 CIP-N, Rapport explicatif, point 3.1, art. 8, al. 1, let. g.

17 CIP-N, Rapport explicatif, point 3.1, art. 8, al. 1, let. g.

18 CIP-N, Rapport explicatif, point 3.1, art. 8, al. 1, let. g.

19 §15a de la loi allemande sur l'asile.

Les personnes requérantes d'asile sont actuellement déjà soumises à une obligation légale de collaborer à la procédure d'asile. Elles ont donc déjà la possibilité de remettre volontairement les données de leur téléphone portable et de leur ordinateur en tant que moyens de preuve, par exemple des photographies documentant leur exil ou leurs correspondances. En outre, le SEM procède déjà à des investigations sur des données plus accessibles, telles que la consultation des profils ouverts au public sur les réseaux sociaux, qui sont tout à fait suffisantes et n'entament en rien le droit à la vie privée. Une expertise LINGUA représenterait également une atteinte moins grande. La finalité évoquée, à savoir l'établissement de l'identité et de la nationalité, peut donc être atteinte de manière adéquate au moyen de mesures moins drastiques, raison pour laquelle la **condition de nécessité n'est pas remplie.**

L'évaluation des supports de données étant prévue au début de la procédure – selon le rapport explicatif durant la phase préparatoire déjà – et compte tenu des contraintes de temps dans la procédure accélérée, il paraît bien peu probable qu'il soit réellement possible de garantir que les mesures moins drastiques pourront être appliquées les premières. C'est pourquoi il convient d'**inscrire dans la loi** cette **graduation des mesures**, à savoir **l'obligation d'appliquer d'abord l'ensemble des mesures qui portent une atteinte moins forte aux droits fondamentaux des personnes requérantes d'asile.**

L'association des avocats allemands (*Deutscher Anwaltverein*) a également estimé que l'introduction d'une telle réglementation en Allemagne était clairement disproportionnée : « L'obligation de collaborer, telle qu'envisagée pour la personne requérante d'asile et le pouvoir d'investigation et d'évaluation qui en résulte sont excessifs. Ils concernent l'ensemble des supports de données – les téléphones mobiles, les smartphones, les tablettes, les ordinateurs portables et autres ordinateurs, les disques durs externes et les clés USB, ainsi que toutes les données de la personne concernée qui y sont contenues – à l'exception des données qui peuvent être attribuées au domaine essentiel de la vie privée. Cela va trop loin compte tenu de la gravité de l'atteinte qui en résulte. En outre, il n'est pas non plus nécessaire de stocker et d'utiliser ce volume de données pour établir l'identité et/ou la nationalité de la personne concernée. Ainsi, de nombreuses données devraient être stockées et consultées sans que cela ne soit nécessaire à la finalité recherchée d'établissement de l'identité et/ou de la nationalité. »[20]

5.3 Données particulièrement sensibles

Selon le nouv. art. 8a al. 1 LAsi de l'avant-projet, les données que le SEM peut traiter comprennent également des données personnelles particulièrement sensibles telles qu'elles sont définies à l'art. 3 let. c LPD. Il s'agit de données concernant les opinions ou activités religieuses, philosophies, politiques ou syndicales ; la santé, la sphère intime ou l'appartenance à une race ; les mesures d'aide sociale ; les poursuites ou sanctions pénales et administra-

[20] Prise de position de l'Association des avocats allemands (*Deutscher Anwaltverein*) par le Comité Gefahrenabwehrrecht (droit à la prévention des risques) sur le projet de loi pour une meilleure application de l'obligation de quitter le pays (BT-Drs. 18/11546), mai 2017, https://dav-migrationsrecht.de/files/page/0_86660500_1497055889s.pdf, p. 3f.

tives. Il convient de se demander pourquoi ces données sont nécessaires pour établir l'identité, la nationalité ou l'itinéraire.[21] Or, il ne peut être exclu que lors de la recherche d'informations concernant l'identité et la nationalité de la personne requérante d'asile, des données particulièrement sensibles soient révélées, alors qu'elles ne font pas explicitement l'objet d'une recherche. On ignore comment seront traitées de telles « découvertes accidentelles ». Du point de vue de l'OSAR, il s'agit là d'un aspect qui met en lumière le caractère sensible de cet avant-projet ainsi que la gravité (inutile) de son atteinte à la protection de la vie privée. Il convient de se demander si l'essence du droit fondamental au respect de la vie privée au sens de l'art. 36 al. 4 Cst. peut être respecté.

Dans le cadre des débats en Allemagne, Pro Asyl a déclaré : « Les smartphones en particulier constituent un dispositif de stockage de données absolument privées, qu'il s'agisse de photos privées ou de conversations intimes. Dans la pratique, il ne sera guère possible à l'Office fédéral de procéder à une consultation des appareils techniques sans accéder directement à des données extrêmement personnelles du cœur de la sphère privée. »[22] Pro Asyl conclut : « La consultation systématique des données des téléphones portables, prévue par le projet de loi, crée des « réfugié de verre », le cœur de la sphère privée, pourtant protégé par la Constitution, n'a plus de frontière. Il s'agit là d'un acte d'espionnage anticonstitutionnel. »[23]

5.4 Un consentement non volontaire

La CIP-N estime que la proposition respecte le principe de proportionnalité en ce sens, notamment, que l'évaluation n'est effectuée qu'avec le consentement des personnes requérantes d'asile. Celles-ci pourraient donc décider elles-mêmes de l'utilisation de leurs données en refusant de les remettre. Or, un refus de remettre des supports de données électroniques constituerait une **violation de l'obligation de collaborer.** Un tel refus aurait de **graves conséquences sur la procédure :**

- Influence négative sur l'examen de la vraisemblance
- Classement informel (art. 8, al. 3bis LAsi)
- Rejet sans audition (uniquement avec octroi du droit d'être entendu) en cas de violation grave et coupable de l'obligation de collaborer (art. 36, al. 1, let. c en lien avec art. 31a, al 4 LAsi)
- Détention administrative en cas de violation de l'obligation de collaborer à la procédure de renvoi (nouv. art. 76 al. 1 let. b no. 3 LEtr)[24]

Compte tenu de ces conséquences, on ne peut parler d'une remise « volontaire » des supports de données ni d'une collaboration au traitement des données à caractère personnel. L'argument de la CIP-N selon lequel l'absence de contrainte atteste de la proportionnalité de la mesure n'est donc pas défendable aux yeux de l'OSAR.

La présence de la personne requérante d'asile pendant l'évaluation ou le respect du droit d'être entendu ne saurait suffisamment atténuer la gravité de l'atteinte au droit fondamental.

---

21 Concernant la protection des données dans ce contexte, voir le point 8 ci-dessous.
22 Pro Asyl, prise de position, 22.03.2017, p. 20.
23 Pro Asyl, prise de position, 22.03.2017, p. 4.
24 Du point de vue de l'OSAR, la détention administrative serait illicite pour cette raison (voir point 7 ci-dessous), mais la CIP-N mentionne la possibilité de mesures contraignantes dans le rapport explicatif, point 3.1, art. 47 al. 2 et 3.

Selon l'art. 4, al. 5, LPD[25], le consentement de la personne concernée au traitement des données à caractère personnel (lorsque celui-ci est requis) n'est valable que si la personne exprime sa volonté librement et après avoir été dûment informée. En outre, lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être explicite. Compte tenu de la complexité des procédures – sélection, sauvegarde temporaire, évaluation et utilisation des données, identification des autorités compétentes et des données à leur transmettre –, il paraît difficilement imaginable que les personnes requérantes d'asile seront suffisamment informées au moment de la remise des supports de données pour pouvoir donner leur consentement éclairé et donc valable à la mesure. Pour ces raisons supplémentaires, il ne peut être question de consentement volontaire. Par ailleurs, il apparaît clairement que la notion de consentement, si elle est abordée dans le rapport explicatif, n'est pas mentionnée dans le projet de loi.

6 Comparaison avec le droit de la procédure pénale

En droit de la procédure pénale, l'évaluation des données des téléphones portables fait l'objet d'une réglementation très restrictive. Les smartphones des auteurs présumés d'infractions ne peuvent être surveillés et analysés qu'en cas de **lourds soupçons laissant présumer qu'une infraction grave a été commise**[26]. Or, en ce qui concerne les personnes requérantes d'asile, de simples doutes quant à leurs déclarations suffiraient désormais à autoriser la consultation des données de leurs téléphones portables et ordinateurs. L'initiative institue ainsi une suspicion généralisée reposant sur le préjugé selon lequel si une personne réfugiée se présente sans passeport, on peut partir du principe qu'elle tente de dissimuler délibérément son identité et ne veut pas collaborer à l'établissement de son identité. Pourtant, de nombreuses raisons peuvent expliquer pourquoi une personne requérante d'asile ne possède pas de passeport. Il arrive ainsi souvent qu'elles n'aient jamais reçu de tels documents dans leur pays d'origine.

En outre, dans les procédures pénales, la surveillance de la correspondance par poste et télécommunication est soumise à une **autorisation du tribunal**[27]. Ainsi, la licéité de la surveillance (y compris son caractère proportionnel) doit être examinée par un tribunal dans un délai de 24 heures. Certes, une fouille peut également être ordonnée par le ministère public. Toutefois, elle doit faire l'objet d'un mandat écrit, sauf cas d'urgence[28]. Une fouille systématique et préventive est par ailleurs exclue[29]. De telles conditions, telles que prévues par le droit de procédure pénale, notamment un contrôle par un tribunal, sont totalement absentes de la présente proposition concernant l'obligation de collaboration dans le cadre des procédures d'asile. Les manquements survenus pourraient au plus tôt être invoqués rétroactivement au stade du recours devant le Tribunal administratif fédéral. Cela serait toutefois trop tard, l'évaluation des données ayant alors déjà été effectuée. **Les personnes requérantes d'asile ne sont pas des criminels présumés**. Il ne peut être justifié qu'une consultation étendue de leurs supports de données soit permise sans **(au moins) les mêmes garanties**

[25] Loi fédérale sur la protection des données, RS 235.1
[26] Cf. art. 269 et ss. du Code de procédure pénale (CPP, RS 312.0) ; les dispositions de la Loi fédérale sur la surveillance par poste et télécommunication (LSCPT, RS 780.1) sont également applicables.
[27] Obligation d'autorisation : art. 272 al. 1 du CCP, procédure d'autorisation : art. 274 CC.
[28] Art. 198 CPP et art. 241 al. 1 CPP.
[29] TAF, arrêt 6B_998/2017 du 20 avril 2018, consid. 2.1.1.

procédurales de base s'appliquant aux personnes soupçonnées d'avoir commis une infraction pénale. La présence ou l'implication de la représentation juridique des personnes requérantes d'asile et le respect du droit d'être entendu ne permettront pas de pallier à cette grave lacune. Il s'agit donc de prévoir un contrôle assuré par un tribunal.

En vue de l'introduction de la réglementation en Allemagne, Pro Asyl a également souligné, se fondant sur la jurisprudence de la Cour constitutionnelle fédérale allemande, que, dans le cadre d'une procédure pénale, une décision judiciaire était nécessaire pour accéder aux données de connexion. Pro Asyl ajoute : « L'établissement de l'identité n'est pas comparable, même de loin, à la situation des enquêtes pour des infractions particulièrement graves. Si même dans ces cas-là le juge est tenu de se prononcer, cela s'applique d'autant plus à des réfugiés innocents, qui ne sont soupçonnés d'aucun crime et n'ont simplement pas de papiers d'identité. »[30]

7 Obligation de collaborer dans la procédure de renvoi

En outre, l'OSAR estime qu'il est problématique que le projet de loi dépasse les exigences de l'initiative parlementaire 17.423 en ce sens qu'il étend l'obligation de collaborer à la procédure de renvoi (nouv. art. 47 al. 2-3 LAsi). Il existe déjà une obligation de collaborer à l'obtention de documents de voyage valables après qu'une décision de renvoi exécutoire ait été prise (art. 8 al. 4 LAsi, qui deviendrait selon l'avant-projet : nouv. art. 47 al. 1 LAsi). En outre, l'identité, la nationalité et l'itinéraire sont établis au début de la procédure d'asile. Compte tenu des graves atteintes à la vie privée, il est donc disproportionné de contraindre (à nouveau) la personne en procédure de renvoi à remettre ses supports de données électroniques et à les faire évaluer par le SEM. En outre, le nouv. art. 47, al. 3, LAsi prévoit que « les données nécessaires à l'exécution du renvoi » peuvent être transmises aux autorités cantonales. Un acteur supplémentaire serait donc impliqué dans la procédure de renvoi, ce qui soulève d'autres problèmes en matière de protection des données.

Aux yeux de l'OSAR, refuser de respecter l'obligation de collaborer en matière de supports électroniques de données dans le cadre de l'exécution du renvoi ne doit pas conduire à une détention administrative. Le projet de loi ne contient d'ailleurs aucune réglementation explicite en ce sens : le nouv. art. 76 al. 1 let. b ch. 3 LEI qui est proposé n'est aucunement modifié sur le fond (il ne renvoie pas au nouv. art. 47 al. 2-3 LAsi proposé, mais au nouv. art. 47 al. 1 LAsi (obligation de collaborer à l'obtention de documents de voyage valables) et non plus à l'art. 8 al. 4 LAsi). A la lumière de la liste explicite des violations de l'obligation de collaborer considérées comme des motifs de détention (art. 90 LEI, art. 8 al. 1 let. a, art. 47 al. 1 LAsi), il apparaît *a contrario* que le refus de remettre ses supports de données *ne* constitue *pas* un motif de détention. Toutefois, selon l'interprétation qui peut être faite de l'obligation de collaborer telle que formulée à l'art. 90 LEI, notamment de l'expression « en particulier », l'OSAR n'exclut pas qu'un refus de collaborer en ce qui concerne la remise de supports de données

[30] Prise de position de PRO ASYL du 27 mars 2017 devant la commission des affaires intérieures du Bundestag allemand sur le projet de loi du gouvernement fédéral : Projet de loi visant à améliorer l'application de l'obligation de quitter le pays, BR Printed Paper 179/17, 22.03.2017, https://www.bundestag.de/resource/blob/500016/c93c5454d698d8b0e8f08117cefae473/18-4-825-A-data.pdf, p. 21.

électroniques puisse, dans des cas individuels, entraîner une mise en détention en vue de l'expulsion[31]. Une telle détention serait disproportionnée.

Si refuser de remettre ses supports de données dans le cadre d'une procédure de renvoi devait en effet exposer la personne concernée à de la détention administrative, on ne pourrait alors parler de mesure *volontaire,* comme cela a déjà été souligné au point 5.4.

8 Protection des données

La procédure d'asile implique le traitement de données sensibles. La protection des données des personnes concernées ainsi que la proportionnalité doivent être respectées à toutes les étapes de la procédure. Pour être introduites, toutes les réglementations doivent au préalable avoir été examinées, évaluées et approuvées par le Préposé fédéral à la protection des données et à la transparence (PFPDT).

Au moment de l'introduction d'une réglementation similaire en Allemagne, le Commissaire fédéral allemand pour la protection des données et la liberté d'information (*deutscher Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) a exprimé de graves inquiétudes en matière de protection des données.[32] La Société pour les libertés civiles (*Gesellschaft für Freiheitsrechte*) a quant à elle estimé que le traitement des données par le BAMF contrevenait « à divers principes du droit de la protection des données, en particulier à la minimisation des données et à l'adéquation des mesures à la finalité, mais aussi à la transparence et à la traçabilité du traitement des données »[33]. En Allemagne, dans trois affaires, encore en cours, des personnes requérantes d'asile ont déposé un recours contre l'évaluation de leurs téléphones mobiles[34]. En Autriche, la base juridique correspondante n'a jusqu'à présent jamais été appliquée, entre autres pour des motifs liés à la protection des données[35]. En Belgique, une base juridique similaire a été introduite, contre l'avis de l'autorité de protection des données[36]. Diverses organisations ont déposé une plainte contre ce règlement[37], qui est en instance devant la Cour constitutionnelle de Belgique. Selon les organisations plaignantes, le règlement n'a encore jamais été mis en œuvre.

---

31 Dans le rapport explicatif, la CIP-N fait également référence à la possibilité de mesures contraignante, section 3.1, art. 47, al. 2 et 3.

32 Andrea Vosshoff, commissaire fédéral allemand à la protection des données et à la liberté d'information, lettre à la commission des affaires intérieures du Bundestag concernant un projet de loi visant à améliorer l'application de l'obligation de quitter le pays, 23.03.2017, https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf.

33 Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 6.

34 https://www.infomigrants.net/en/post/24574/migrants-sue-german-state-over-mobile-phone-searches. L'article met en lumière ce qu'implique une telle mesure pour les personnes concernées. L'une d'elles déclare ainsi : «It felt like I was handing over my whole life.»

35 Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 44.

36 Commission de la protection de la vie privée, Avis n° 57/2017 du 11 octobre 2017, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_57_2017_0.pdf.

37 Cf. Ciré, Recours contre la réforme « Mammouth », https://www.cire.be/recours-contre-la-reforme-mammouth/.

L'avant-projet soulève diverses questions relatives à la protection des données, par exemple en ce qui concerne les informations fournies à la personne concernée et son consentement[38], la sauvegarde temporaire prévue des données (nouv. art. 8a al. 3 LAsi) et leur transmission à d'autres autorités (autorités de sécurité selon l'art. 22a Lpers / art. 20 al. 3 et 4 LRens ; autorités cantonales, nouvel art. 47 al. 3 LAsi), l'implication de tiers pour le recueil de supports de données (art. 26 al. 5 LAsi) ainsi que l'implication de données appartenant à des tiers. Or, les explications fournies en la matière par le rapport explicatif sont trop brèves et ne suffisent pas à dissiper les inquiétudes concernant la protection des données. Une analyse et une justification plus détaillées seraient en effet nécessaires.

Selon le nouv. art. 8a al. 1 LAsi de l'avant-projet, les données que le SEM est autorisé à traiter comprennent également des données personnelles particulièrement sensibles au sens de l'art. 3 let. c LPD. Il s'agit de données sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales ; sur la santé, la sphère intime ou l'appartenance à une race ; sur les mesures d'aide sociale ; sur les poursuites ou sanctions pénales et administratives. Le traitement et l'utilisation de ces données vont bien au-delà de la finalité d'établissement de l'identité et portent donc atteinte à l'un des principes centraux de la protection des données : le principe de la finalité, et ce, dans un domaine où il existe un besoin particulier de protection des données.[39] L'OSAR demande donc une restriction explicite en matière d'utilisation et d'évaluation des informations à des données qui servent effectivement et exclusivement à l'établissement de l'identité.

L'avant-projet (nouv. art. 8a, al. 5, LAsi) prévoit que le Conseil fédéral détermine quelles données seront relevées et règle les modalités d'accès aux données personnelles et de leur analyse. Il détermine en particulier les différentes données électroniques qui peuvent être analysées. L'OSAR estime qu'il ne suffit pas de déléguer au Conseil fédéral les pouvoirs législatifs en matière de sécurité et de protection des données, car les exigences en matière de densité normative sont particulièrement élevées en ce qui concerne le traitement de données présentant un potentiel de risque aussi élevé que dans le cas présent. Aux yeux de l'OSAR, les éléments fondamentaux du domaine délégué devraient donc être précisés par la loi.

9 Coûts

Le rapport explicatif de la CIP-N ne contient que des informations vagues sur les coûts prévus. En conséquence, il n'est pas encore possible d'évaluer les dépenses liées au personnel requis et les coûts liés à l'acquisition, à l'installation et à l'exploitation de nouveaux composants informatiques ainsi qu'aux interprètes et à l'implication de la représentation juridique. Selon de « premières demandes informelles du SEM à différents fournisseurs de logiciels d'analyse, les coûts d'acquisition des composants nécessaires se situent entre 100 000 et

[38] Voir le point 5.4 ci-dessus.

[39] Cf. Peter Uebersax: Zur Revision des Ausländergesetzes gemäss der Botschaft des Bundesrates vom März 2018, in: Jusletter 9.7.2018; Caroline Gloor Scheidegger, Adrian Lobsiger: Rechtliche Fragen bei der Bearbeitung von Migrationsdaten, in: Stephan Breitenmoser, Otto Lagodny, Peter Uebersax (Hrsg.): Schengen und Dublin in der Praxis – aktuelle Herausforderungen, Zürich 2018, pp. 317-338.

200 000 francs. »[40] Le manque de précision de ces informations jette toutefois de sérieux doutes sur la fiabilité de ces estimations.

À titre de comparaison : en Allemagne, les coûts liées au matériel et aux logiciels nécessaires ainsi qu'à l'analyse des données se sont révélés nettement supérieurs aux estimations formulées : de 2017 à avril 2018, les coûts s'élevaient à 7,6 millions d'euros, soit un montant deux fois plus élevés que les estimations initiales[41]. La Société pour les libertés civiles (*Gesellschaft für Freiheitsrechte*) souligne d'ailleurs : « Selon les informations fournies en décembre 2018 par le ministère fédéral de l'Intérieur, un coût total de 11,2 millions d'euros est prévu d'ici fin 2019 pour le système. Les coûts totaux continueront à augmenter, et les coûts de maintenance devraient s'élever à quelque 2,1 millions d'euros par an. En outre, 300 000 euros par an pour les licences sont prévus conformément à l'exposé des motifs de la loi. ».[42] La Société pour les libertés civiles (*Gesellschaft für Freiheitsrechte*) conclut ainsi : « Les fabricants de technologies de surveillance seront les premiers bénéficiaires [de la loi], qui tireront de gros profits avec leurs offres ».[43]

Les coûts élevés prévus ne sont pas justifiés compte tenu des bénéfices limités attendus[44]. Pour cette raison également, la modification proposée apparaît disproportionnée et inutile aux yeux de l'OSAR.

[40] CIP-N, Rapport explicatif, point 4.1.

[41] Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 34.

[42] Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 35.

[43] Gesellschaft für Freiheitsrechte, Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, Dezember 2019, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf, p. 47.

[44] Voir le point 5.1 ci-dessus.