



17.423

Initiative parlementaire

Obligation de collaborer à la procédure d'asile. Possibilité de contrôler les téléphones mobiles

Rapport de la Commission des institutions politiques du Conseil national

du 16 octobre 2020

Madame la Présidente,
Mesdames, Messieurs,

Par le présent rapport, nous vous soumettons le projet d'une modification de la loi sur l'asile que nous transmettons simultanément au Conseil fédéral pour avis.

La commission propose d'accepter le projet d'acte ci-joint.

16 octobre 2020

Pour la commission:

Le président, Andreas Glarner

Condensé

L'absence de documents permettant d'établir l'identité des requérants d'asile ralentit et complique la procédure d'asile. La Commission des institutions politiques du Conseil national (CIP-N) est d'avis que l'analyse des supports de données mobiles tels que téléphones portables ou tablettes constitue une méthode efficace pour obtenir des informations sur l'identité d'une personne.

D'autres pays procèdent déjà de cette manière en vue de déterminer l'identité des personnes concernées. Il n'y a pas de raison que la Suisse ne puisse pas en faire autant.

En conséquence, la CIP-N propose de modifier la loi sur l'asile de manière à accorder au Secrétariat d'État aux migrations des compétences étendues pour procéder au contrôle des supports de données mobiles en vue d'établir l'identité des requérants d'asile. L'obligation de collaborer faite aux requérants d'asile sera donc élargie en ce sens.

Rapport

1 Contexte

1.1 Mesures à prendre

L'initiative parlementaire déposée par le conseiller national Gregor Rutz le 17 mars 2017 demande que les bases légales soient modifiées de sorte que lorsque l'identité du requérant ne pourra pas être établie par d'autres moyens, l'obligation de collaborer faite aux requérants d'asile comprendra aussi l'obligation de remettre les supports de données mobiles; symétriquement, les compétences des autorités comprendront aussi le droit de contrôler ces appareils.

Dans son développement, l'auteur de l'initiative constate qu'un nombre considérable de requérants d'asile entrent en Suisse sans papiers permettant d'établir leur identité. Ces circonstances ralentissent et compliquent la procédure d'asile. Souvent, ces personnes possèdent néanmoins des supports de données mobiles comme un téléphone portable ou une tablette. Ces appareils contiennent un grand nombre de données pouvant être utiles pour établir l'identité de leurs propriétaires.

Conformément au droit en vigueur, le Secrétariat d'État aux migrations n'a aucun moyen de vérifier le contenu des supports de données mobiles pour en tirer des indications supplémentaires quant à l'identité d'un requérant d'asile.

1.2 Solutions étudiées et solution retenue

La CIP-N a donné suite à l'initiative le 1^{er} février 2018 par 17 voix contre 7. Le 21 juin 2018, son homologue du Conseil des États s'est ralliée à cette décision par 9 voix contre 1 et 2 abstentions. Une minorité de la commission juge toutefois que cette méthode est trop contraignante et qu'elle constitue une atteinte excessive à la sphère privée des intéressés.

Les Commissions des institutions politiques des deux conseils ont souscrit aux arguments de l'auteur de l'initiative, qui juge nécessaire que la loi prévoie des possibilités élargies de contrôler les supports de données mobiles en vue de l'établissement de l'identité. L'analyse des données mobiles peut s'avérer une méthode efficace pour obtenir des informations sur l'identité d'une personne. Il apparaît que cette manière de procéder est déjà appliquée dans d'autres pays, notamment en Allemagne. Par ailleurs, la clarification rigoureuse de l'identité des requérants par l'État permet également de renforcer la confiance de la population à l'égard de la procédure d'asile.

1.3 Comparaison avec le droit d'autres États européens

Dans différents autres États européens, les supports électroniques de données sont déjà mis à contribution dans le cadre de la procédure d'asile, en particulier pour

obtenir des informations sur l'identité d'une personne. Ces informations servent également à répondre à des questions se rapportant à la sécurité et à la santé publiques. D'autre part, les données peuvent contribuer à déterminer l'itinéraire des requérants d'asile et la crédibilité de leurs déclarations dans le cadre de la procédure d'asile. Les expériences faites dans d'autres pays ont été prises en compte dans l'élaboration du présent avant-projet. Les bases juridiques en vigueur dans certains pays européens et les méthodes appliquées dans ceux-ci sont brièvement récapitulées ci-après¹.

Au Danemark, en Allemagne, en Finlande et aux Pays-Bas, des bases légales spécifiques permettent de consulter les supports de données mobiles des requérants d'asile. La Belgique possède aussi des dispositions analogues, mais qui n'autorisent l'extraction de ces données qu'avec le consentement du requérant. En Pologne, la loi permet uniquement de contrôler ces appareils dans le cadre d'investigations sur des questions de sécurité ou d'enquêtes pénales.

La conservation des données est un aspect important, mais aussi très controversé. Les pays observés abordent également cette question de différentes manières. La Belgique, le Danemark et l'Irlande n'ont pas encore réglementé la durée de conservation des données et sont en train d'élaborer une base légale tenant compte du Règlement européen sur la protection des données. En Allemagne, ces informations peuvent être consignées dans le dossier du requérant d'asile. Elles sont conservées et supprimées conformément aux délais de conservation usuels du dossier d'asile. La Pologne garde les données extraites à titre de moyens de preuve. Elle ne les détruit pas, à l'exception des informations relatives à des enquêtes pénales, qui ne sont pas conservées au-delà d'un an.

S'agissant du moment auquel les supports de données sont contrôlés, la Belgique, le Danemark et l'Allemagne effectuent en principe l'extraction des données au début de la procédure d'asile, c'est-à-dire dès l'enregistrement des requérants ou lors du premier interrogatoire. En Irlande, cette mesure intervient lors de la première rencontre entre les autorités et le requérant. Au Pays-Bas, les données peuvent être extraites à tout moment, en fonction des besoins.

Reste à clarifier la question de l'autorité habilitée à extraire les données ou à les transmettre à d'autres. De manière générale, l'extraction des données est effectuée soit par les autorités compétentes en matière de migration (Belgique, Irlande), soit par la police (Pays-Bas). La compétence en la matière est parfois partagée par les différentes autorités. En Finlande, par exemple, c'est la police qui se charge de l'extraction des données, le service des migrations étant autorisé à y accéder en cas de besoin. En Belgique, ce sont les autorités en charge de la migration qui les prélèvent et qui les partagent avec la première instance de recours.

¹ Sur la base de l'enquête menée en 2018 par l'IGC (Intergovernmental Consultations on Migration, Asylum and Refugees) en Allemagne, en Belgique, au Danemark, en Finlande, en Irlande, aux Pays-Bas, en Pologne et en Suisse.

1.4 Mise en œuvre de l’initiative par la CIP-N

À sa séance du 21 juin 2018, la CIP-N a chargé son secrétariat et l’administration d’élaborer un avant-projet d’acte. Le 14 février 2020, la commission a approuvé cet avant-projet, en vue de la consultation, par 17 voix contre 8.

1.5 Résultats de la consultation

La commission a mené une consultation du 20 février au 4 juin 2020.

Les avis recueillis sont au nombre de 53. En tout, 25 cantons, cinq partis politiques, deux organisations faîtières de l’économie et 21 autres milieux intéressés se sont exprimés. Parmi les cantons, 24 soutiennent le projet, tandis que Neuchâtel le rejette. Pour ce qui est des partis politiques, l’UDC, le PLR et le PDC soutiennent le projet, le PS et le PES le rejettent. Parmi les organisations qui se sont exprimées sur le projet, l’Union suisse des arts et métiers approuve les modifications de la loi proposées, l’Union syndicale suisse les désapprouve. La grande majorité des autres milieux intéressés qui ont participé à la consultation rejette le projet. La Conférence des directrices et directeurs des départements cantonaux de justice et police, l’Union des villes suisses et l’Association suisse des Magistrats de l’ordre judiciaire ont explicitement renoncé à prendre position.

Dans les réactions critiques, un des arguments avancés est que l’analyse proposée de supports électroniques de données constituerait une atteinte grave aux droits fondamentaux des intéressés. La procédure proposée serait disproportionnée au vu cette atteinte, mais aussi compte tenu du rapport entre son coût et son utilité. Les bases légales proposées sont en outre considérée comme insuffisantes, notamment pour ce qui est du maniement de données personnelles de tiers. À l’opposé de ces critiques, certains participants à la consultation estiment que les modifications législatives proposées ne vont pas assez loin. Certains cantons, en particulier, exigent que la loi prévoie que les supports électroniques de données puissent être saisis sans le consentement de leur détenteur.

2 Grandes lignes du projet

2.1 Nouvelle réglementation proposée

Ces dernières années, la Suisse a enregistré chaque mois entre 1000 et 1500 nouvelles demandes d’asile. L’identité de 70 à 80 % des requérants est inconnue ou ne peut pas être déterminée avec certitude. La Suisse est tenue de respecter la Convention de Genève relative au statut des réfugiés et veille au bon fonctionnement de son système d’asile. Ce faisant, elle doit veiller à ce que le droit à l’asile soit accordé aux personnes qui ont réellement besoin de cette protection. L’établissement de l’identité est un aspect important pour mener à bien cette mission. Dans ce contexte, l’obligation de collaborer du requérant est essentielle (art. 8 de la loi sur l’asile, LAsi). Le présent avant-projet de loi élargit cette obligation. Dans le même temps, il étend les compétences des autorités qui peuvent, en l’absence d’autres moyens pour établir

l'identité du requérant, se saisir aussi des supports de données mobiles de cette personne.

Le Secrétariat d'État aux migrations a réalisé un projet pilote de novembre 2017 à mai 2018 dans deux centres d'enregistrement et de procédure fédéraux (Chiasso et Vallorbe). Dans le cadre de ce projet, les supports de données mobiles de requérants d'asile ont été utilisés avec le consentement de ceux-ci en vue de leur identification. Il a ainsi été possible d'obtenir des informations utiles sur l'identité des requérants concernés, leur origine et leur itinéraire. De plus, des informations importantes ont pu être transmises aux autorités de police et de sécurité. Les résultats de ce projet pilote ont été pris en compte dans la décision relative au présent avant-projet et lors de l'élaboration de ce dernier.

L'une des mesures principales vise en particulier l'art. 8, LAsi, qui règle l'obligation de collaborer du requérant dans la procédure d'asile. Cet article doit être complété d'une nouvelle lettre g, qui prévoit que les supports électroniques de données tels que téléphones portables ou tablettes (cf. art. 8a, al. 2, P-LAsi) doivent être temporairement remis au Secrétariat d'État aux migrations lorsque l'identité, la nationalité et l'itinéraire de la personne concernée ne peuvent être établis sur la base de papiers d'identité ou d'une autre manière. Cela signifie aussi qu'il faut toujours d'abord donner au requérant la possibilité de fournir, de son propre chef, des informations sur sa nationalité, son identité ou son itinéraire.

La mesure proposée peut également contribuer à lutter contre les activités des passeurs et à obtenir des informations utiles à l'élucidation de crimes de guerre.

La protection de la sphère privée est un droit fondamental important, qui doit bien entendu aussi être accordé dans la procédure d'asile. L'inspection des supports de données mobiles du requérant constitue une atteinte à sa sphère privée. Une entorse à ce droit fondamental n'est justifiée qu'à certaines conditions: il faut pour cela qu'une base légale et un intérêt public existent, que l'atteinte soit proportionnée et que l'essence même du droit fondamental soit préservée. La commission considère que ces critères sont remplis, étant donné notamment qu'il n'y a pas, en l'espèce, d'atteinte disproportionnée à la sphère privée. La consultation des supports de données mobiles n'intervient que si les autres moyens ont été épuisés; il n'est par ailleurs pas prévu de saisir les supports de données mobiles des personnes concernées sans leur consentement (voir commentaire de l'art. 8, al. 1, let. g). La commission juge également justifié la sauvegarde temporaire des informations, afin de garantir une évaluation aussi efficace que possible.

La CIP-N est convaincue que cette mesure simplifiant l'établissement de l'identité des requérants est absolument proportionnée au travail qu'elle implique.

Trois ans après l'entrée en vigueur du projet, un rapport d'évaluation devra être établi, lequel devra fournir des informations sur la mise en œuvre de cette modification législative et ses effets (cf. dispositions finales).

Suite à la consultation, une minorité de la commission (Glättli, Barrile, Funicello, Gysin Greta, Kälin, Marra, Marti Samira, Widmer Céline) s'est prononcée contre le projet et propose de ne pas entrer en matière. Elle estime que l'analyse de supports électroniques de données constitue une atteinte grave aux droits fondamentaux des intéressés et qu'elle est de ce fait disproportionnée. Elle considère aussi que les

application de l'art. 8, al. 3^{bis}, LAsi ou à son rejet en application de l'art. 31a, al. 4, LAsi (en relation avec l'art. 36, al. 1, let. c, LAsi).

Le but de la nouvelle réglementation est avant tout de pouvoir récupérer sur un support électronique de données des indications directement exploitables (par ex. une photographie d'une pièce d'identité).

Même des indications qui ne sont pas directement exploitables, comme l'itinéraire ou les données de contacts, peuvent aussi fournir des éléments pour établir l'identité de la personne.

Les dispositions selon les art. 102f ss LAsi relatives à la protection juridique dans les centres de la Confédération s'appliquent aussi à l'analyse des supports électroniques de données. Le représentant juridique doit par conséquent être informé dès le départ de toutes les démarches.

Une minorité (Rutz Gregor, Addor, Bircher, Glarner, Marchesi, Steinemann) exige que les supports électroniques de données puissent être saisis sans le consentement de leur détenteur.

Al. 4

Pour des raisons de systématique, cet alinéa doit être déplacé à l'art. 47, al. 1, P-LAsi, puisqu'il traite de l'obligation de collaborer à la procédure de renvoi.

Art. 8a Traitement de données issues de supports électroniques de données

Al. 1

Cette disposition règle le traitement des données personnelles recueillies sur les supports électroniques de données. Le traitement visé à l'art. 8a P-LAsi sera possible pendant toute la durée de la procédure de première instance. Dans la pratique, des indices rendant nécessaires un contrôle du support électronique de données peuvent apparaître à tout moment dans la procédure. Des déclarations faites à un moment donné peuvent aussi se révéler fausses par la suite (par ex. une carte d'identité est en fait falsifiée). L'analyse d'un support électronique de données peut donc aussi n'intervenir qu'au moment de l'audition sur les motifs d'asile. La remise et l'analyse de supports électroniques de données dans le cadre de la procédure de renvoi sont régies par l'art. 47, al. 2, P-LAsi. Peuvent aussi être traitées les données personnelles qui ne sont pas directement sur le support mais sont enregistrées dans un espace «virtuel», c'est-à-dire qu'elles se trouvent dans un nuage informatique ou des services en ligne.

Al. 1^{bis}

Ne peuvent en principe être traitées que les données personnelles du requérant lui-même. Les données personnelles de tiers ne peuvent être traitées que si les données du requérant ne suffisent pas à clarifier son identité, sa nationalité ou son itinéraire.

Pour une minorité de la commission (Barrile, Funicello, Glättli, Gysin Greta, Marra, Marti Samira, Kälin, Widmer Céline), le traitement de données personnelles de tiers va trop loin. Elle rejette cette disposition.

Al. 2

La norme définissant les types de support électronique de données n'est pas formulée de manière exhaustive afin de pouvoir tenir compte des progrès à venir de la technologie.

Al. 2bis

L'analyse de supports électroniques de données ne doit intervenir que si l'identité, la nationalité ou l'itinéraire d'un requérant d'asile ne peuvent être établis par d'autres moyens appropriés (par ex. sur la base de documents d'identité). En raison de la gravité de l'atteinte à la sphère privée de l'intéressé et du grand travail que nécessite l'analyse de ces supports de données, il convient d'évaluer soigneusement au préalable, dans chaque cas, si cette analyse est nécessaire et proportionnée. Pour cette évaluation préalable, on tiendra compte des déclarations de la personne concernée et d'éventuels documents pouvant être pertinents pour la procédure.

Une minorité (Rutz Gregor, Addor, Binder, Bircher, Buffat, Glarner, Jauslin, Marchesi, Romano, Steinemann) considère que cette disposition est inutile.

Al. 3

Le but de cette sauvegarde temporaire est de mettre les données en lieu sûr jusqu'à leur analyse tout en permettant au requérant de continuer à utiliser son téléphone mobile ou tout autre support. Les données personnelles peuvent être sauvegardées temporairement sur un serveur sécurisé du Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP) ou du SEM, où elles resteront jusqu'à leur analyse (al. 4).

Al. 3bis

Au vu de la gravité de l'atteinte à la sphère privée de la personne concernée, il est indispensable de l'informer de manière complète des détails de l'analyse de supports électroniques de données. Ces explications doivent porter sur le but de la mesure, sur la nature des données qui seront traitées, sur la manière dont l'analyse sera effectuée et sur ce qu'il adviendra des données en question (sauvegarde, effacement, etc.). Ce devoir d'information sert à garantir les droits de la personne concernée durant la procédure et à maintenir le rapport de confiance nécessaire à son bon déroulement.

Une minorité (Gregor Rutz, Addor, Binder, Bircher, Buffat, Marchesi, Glarner, Jauslin, Romano, Steinemann) rejette cette disposition.

Al. 4 et 5

Il n'est pas permis d'accéder aux données jusqu'au début de l'analyse. Le collaborateur compétent du SEM ne peut accéder aux données personnelles aux fins de l'analyse que lorsque les personnes concernées sont présentes, sauf si ces dernières renoncent expressément à être présentes lors de l'analyse (par exemple au moyen d'une déclaration de renonciation écrite). L'accès du SEM est aussi possible aux fins de l'analyse si le requérant refuse d'être présent lors de l'analyse.

L'analyse se limite aux données personnelles, y compris les données sensibles, qui se rapportent au requérant et qui peuvent être utilisées dans la procédure d'asile, par exemple des données susceptibles de fournir des indications sur l'identité de la personne ou sur l'itinéraire qu'elle a emprunté concernant l'analyse de données

personnelles de tiers, voir le commentaire de l'al. 1^{bis}). Un procès-verbal est établi. La transmission des données personnelles n'est possible qu'en vertu d'une base légale au sens formel. Ce cas peut se produire dans la pratique lorsque l'analyse met au jour des indices d'une infraction ou d'une menace grave pour la sécurité intérieure ou extérieure de la Suisse.

L'analyse est en principe effectuée durant la phase préparatoire, dès lors que la mesure est utile et possible, mais on peut aussi envisager de la réaliser pendant l'audition sur les motifs d'asile. Les données personnelles doivent être effacées une fois l'analyse terminée. Elles sont automatiquement effacées un an au plus après leur sauvegarde temporaire.

Afin de faciliter son travail d'analyse, le SEM peut utiliser des outils informatiques (logiciels) lui permettant en particulier de trier les données. Le but est de circonscrire l'analyse aux seules données pertinentes pour identifier le requérant. Sur le plan technique, il faut veiller à ce qu'aucune donnée ne soit enregistrée durant cette phase. Le Conseil fédéral fixe dans une ordonnance les modalités de ce tri (al. 5, cf. ch. 4.1). Par ailleurs, le Conseil fédéral détermine quelles données sont relevées selon l'al. 1 et règle les modalités de l'accès aux données et de leur analyse.

L'analyse des données se fait en présence du requérant d'asile et de son représentant juridique, pour autant que le requérant n'ait pas renoncé à être présent lors de l'analyse, ou refusé de l'être (voir à ce sujet l'art. 102j, al. 2, LAsi). Le requérant peut se prononcer sur l'analyse qui est faite de ses données personnelles. Le droit d'être entendu est ainsi garanti (cf. al. 6).

Si aucune donnée n'a été sauvegardée temporairement, par exemple parce qu'un support de données n'est apparu qu'ultérieurement, l'analyse peut se faire par consultation directe du support de données pendant une audition (cf. al. 4, dernière phrase).

Une minorité de la commission (Barrile, Funiciello, Flach, Glättli, Gredig, Gysin Greta, Marra, Marti Samira, Kälin, Widmer Céline) souhaite que les données soient effacées six mois au plus après leur sauvegarde temporaire.

Al. 6

Outre le procès-verbal de l'analyse, sont aussi conservées dans le dossier d'asile par exemple des copies de papiers d'identité ou des listes d'adresses issues des supports de données contrôlés, pour autant que ces informations puissent être utilisées dans la procédure d'asile. Le requérant peut faire usage de son droit à consulter le dossier et se prononcer sur l'analyse qui a été faite de ses données personnelles. Son droit d'être entendu est ainsi garanti.

Art. 47 Obligation de collaborer dans le cadre de la procédure de renvoi

Al. 1

L'al. 1 reprend, sans modification matérielle, le libellé de l'actuel art. 8, al. 4, LAsi.

Al. 2 et 3

Cette disposition va plus loin que ne le demande l'initiative parlementaire 17.423 et étend la remise et l'analyse de supports électroniques de données à l'exécution des

renvois dans le domaine de l'asile. S'il n'est pas possible, dans le cadre de l'exécution du renvoi, d'obtenir un document de voyage valide dans un délai adéquat, moyennant des mesures appropriées, avant l'entrée en force de la décision d'asile et de renvoi, il faut pouvoir obliger la personne à remettre un support électronique de données. Une confiscation du support électronique de données par le SEM, c'est-à-dire la saisie du dispositif sans le consentement de la personne, n'est cependant pas prévue.

La procédure est réglée de la même manière que la procédure selon l'art. 8a P-LAsi. Cela signifie en particulier que la personne doit avoir la possibilité de se prononcer sur l'analyse qui est faite de ses données, que les données analysées sont consignées dans le dossier d'asile et qu'il est établi un procès-verbal. L'analyse des données est du ressort du SEM, qui y procède soit directement, soit à la demande du canton chargé d'exécuter le renvoi, au titre de l'assistance aux autorités d'exécution conformément à l'art. 71 de la loi fédérale sur les étrangers et l'intégration (LEI).

Le refus de la personne de remettre ses supports électroniques de données n'a plus de conséquences sur la procédure à ce stade puisqu'elle est close. Le refus peut néanmoins être assimilé à une violation de l'obligation de collaborer justifiant l'application de mesures de contrainte selon les art. 73 ss LEI (cf. art. 76, al. 1, let. b, ch. 3, P-LEI).

La communication de données personnelles analysées aux pays d'origine ou de provenance, à des États tiers ou à des organisations internationales est régie par les art. 97 et 98 LAsi.

Une minorité (Rutz Gregor, Addor, Bircher, Glarner, Marchesi, Steinemann) exige que dans la procédure de renvoi, il soit possible de saisir les supports électroniques de données sans le consentement de leur détenteur.

Al. 4

L'al. 4 reprend, sans modification matérielle, le libellé de l'actuel art. 47 LAsi.

Art. 96, al. 1

Adaptation rédactionnelle (abréviation de la loi fédérale sur la protection des données, LPD).

Dispositions finales

Lors de la consultation, plusieurs participants ont demandé qu'il soit inscrit dans la loi qu'un rapport d'évaluation sur l'efficacité des mesures d'analyse serait rédigé, comme le mentionnait le rapport explicatif sur l'avant-projet. La disposition finale a cet effet prévoit un rapport unique du Conseil fédéral au Parlement, qui sera présenté au plus tard trois ans après l'entrée en vigueur de la modification législative.

3.2 Loi fédérale sur les étrangers et l'intégration

Art. 76, al. 1, let. b, ch. 3

Adaptation du renvoi (art. 47, al. 1, P-LAsi en lieu et place de l'art. 8, al. 4, LAsi). Voir le commentaire de l'art. 47 P-LAsi.

Art. 90, let. d

Une minorité (Rutz Gregor, Addor, Bircher, Buffat, Glarner, Marchesi, Steinemann) exige que l'analyse des données soit étendue aux personnes du domaine des étrangers.

4 Conséquences pour les finances et le personnel

4.1 Conséquences pour la Confédération

Les auteurs du rapport sur le projet pilote mené par le SEM (cf. également ch. 2.1) relèvent que la procédure testée dans les anciens CEP de Chiasso et de Vallorbe pour analyser le contenu de supports électroniques de données a entraîné un surcroît de travail que les effectifs existants ont pu absorber compte tenu du faible nombre de demandes d'asile. Des ressources en personnel supplémentaires seraient néanmoins nécessaires si la démarche était étendue aux six centres de la Confédération assumant des tâches de procédure et en cas de hausse notable du nombre de demandes d'asile. À la différence de la procédure testée, le projet proposé prévoit que le SEM pourra, à la demande des cantons, analyser le contenu de supports électroniques de données d'anciens requérants d'asile aux fins de l'exécution du renvoi. Ce contrôle, qui devra aussi en principe se faire en présence de l'intéressé, alourdira la charge de travail du SEM. Dans la mesure du possible, cette charge supplémentaire devra être compensée à l'interne.

La question des effectifs supplémentaires qui seront véritablement nécessaires pour analyser le contenu des supports électroniques de données dépend de divers autres facteurs, comme les modalités techniques de mise en œuvre s'agissant notamment de la sauvegarde temporaire des données ou les possibilités concrètes de centraliser certains processus.

Le SEM n'est par conséquent pas en mesure à ce stade de chiffrer précisément les charges de personnel à prévoir. Cet élément sera examiné en détail lors de la définition des dispositions d'exécution, lorsque les modalités techniques de mise en œuvre et le déroulement de la procédure auront été clarifiés.

Le contrôle des supports électroniques de données va entraîner des coûts supplémentaires pour la Confédération pour l'acquisition, la mise en place et l'exploitation de nouveaux composants informatiques, ainsi que pour les prestations d'interprétariat supplémentaires et la participation des représentants juridiques. Il n'est pas non plus possible pour l'heure de détailler ces coûts. 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 200 000 francs.

Au vu des enseignements tirés lors du projet pilote du SEM et des expériences recueillies par d'autres États analysant le contenu de supports électroniques de données dans les procédures relevant du domaine de l'asile, cette nouvelle possibilité d'exploiter des données permettra très vraisemblablement à terme de réaliser des économies, notamment en matière d'exécution des renvois.

4.2 Conséquences pour les cantons et les communes

Ce projet de loi n'entraîne pas de coûts supplémentaires pour les cantons et les communes.

5 Aspects juridiques

5.1 Constitutionnalité

Le projet de modification de la LAsi est fondé sur l'art. 121, al. 1, Cst. (compétence législative de la Confédération en matière d'octroi de l'asile et en matière de séjour et d'établissement des étrangers). Il est conforme à la Constitution fédérale.

5.2 Compatibilité avec les engagements internationaux de la Suisse

Le projet de loi est compatible avec le droit international en vigueur.

L'art. 8 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)³ ainsi que l'art. 17 du Pacte international du 16 décembre 1966 relatif aux droits civils et politiques (Pacte II)⁴ garantissent à toute personne le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir une ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence repose sur une loi et qu'elle constitue, notamment, une mesure nécessaire à la sécurité publique ou à la défense de l'ordre (art. 8, al. 2, CEDH). Le projet de loi ne prévoit pas d'ingérence disproportionnée de l'État dans la sphère privée des requérants d'asile. Il est formulé de telle manière que le requérant d'asile peut décider librement dans quelle mesure il entend collaborer à l'établissement de son identité en acceptant ou en refusant une analyse de ses données personnelles contenues sur un support électronique lui appartenant (cf. commentaire de l'art. 8, al. 1, let. g, P-LAsi).

³ RS 0.101

⁴ RS 0.103.2

5.3 Forme de l'acte à adopter

Au vu de l'objet, du contenu et de la portée du projet, il est indispensable, selon l'art. 164, al. 1, Cst., d'édicter les dispositions relatives à l'examen des données personnelles des requérants d'asile figurant sur des supports électroniques de données sous la forme d'une loi fédérale (modification de la LA_{Si}).

5.4 Frein aux dépenses

Le projet ne contient pas de dispositions relatives aux subventions et ne prévoit ni crédits d'engagement ni plafonds de dépenses. Il n'est donc pas soumis au frein aux dépenses (art. 159, al. 3, let. b, Cst.).

5.5 Conformité à la loi sur les subventions

Le projet ne prévoit pas d'aides financières ni d'indemnités. Il n'est donc pas soumis aux principes de la loi sur les subventions.

5.6 Délégation de compétences législatives

L'art. 8a, al. 5, P-LA_{Si} prévoit que le Conseil fédéral détermine quelles données sont relevées et règle les modalités de l'accès aux données et de leur analyse. Il définira en particulier les différentes données électroniques qui peuvent faire l'objet d'une évaluation (par ex. des données GPS, des numéros de téléphone, etc.).

Le destinataire des modifications d'ordonnances relatives à l'analyse des données personnelles est le SEM.

5.7 Protection des données⁵

En vertu des art. 17 et 19, al. 1, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)⁶, un organe fédéral n'est en droit de traiter et de communiquer des données sensibles que s'il existe une base légale au sens formel. L'art. 8a P-LA_{Si} prévoit la possibilité pour le SEM de traiter les données personnelles figurant sur un support électronique de données appartenant à un requérant d'asile. Une éventuelle communication à un tiers des données personnelles ayant fait l'objet d'une évaluation n'est possible que si elle repose sur une base légale explicite (cf. commentaire de l'art. 8a). On peut mentionner, par exemple, la communication de données personnelles aux autorités de poursuite pénale en cas de crime ou de délits

⁵ Ce chapitre est basé sur le droit applicable. La révision totale de la loi sur la protection des données a été adoptée par le Parlement lors du vote final le 25 septembre 2020.

⁶ RS 235.1

poursuivis d'office (art. 22a LPers) ou d'atteinte grave à la sécurité intérieure ou extérieure de la Suisse (art. 20, al. 3 et 4, LRens).

En application de l'art. 4, al. 3 et 4, LPD, il y a lieu de définir la finalité du traitement envisagé de manière précise et reconnaissable pour les personnes concernées. Le projet autorise le SEM à demander à un requérant d'asile la remise d'un support électronique de données en vue d'établir son identité, sa nationalité ou son itinéraire (art. 8a, al. 1, P-LAsi). Le projet définit clairement les données personnelles qui peuvent faire l'objet d'une analyse, à savoir toutes les informations qui se rapportent à une personne identifiée, selon la définition de l'art. 3, let. a, LPD, ainsi que toutes les données sensibles au sens de l'art. 3, let. c, LPD; il s'agit ici notamment des opinions ou activités religieuses ou politiques, de la santé ou encore de l'appartenance à une race.

