Fouille numérique des demandeurs d'asile. Et la protection de la vie privée ?

Julie Mont[1]

La loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers a été récemment modifiée par la loi du 21 novembre 2017, entrée en vigueur le 22 mars 2018. S'agissant de la procédure d'asile, le législateur a notamment prévu que, désormais, si les instances chargées de l'examen de la demande d'asile ont de bonnes raisons de penser que le demandeur d'asile retient des informations qui sont pourtant pertinentes au stade de l'examen de la demande, elles peuvent l'inviter à produire ces informations, quel que soit le support sur lequel elles se trouvent. Il s'agit d'une nouvelle possibilité de « fouille numérique » du demandeur d'asile, puisque son GSM, son ordinateur, ses profils de réseaux sociaux, …, peuvent ainsi être passés au crible. Si le législateur fonde cette nouveauté sur le consentement de la personne concernée, la validité du consentement du demandeur d'asile s'avère relativement bancale au regard de la législation en matière de protection des données à caractère personnel, et notamment le Règlement européen sur la protection des données, qui est entré en vigueur le 25 mai 2018.

• • •

The Law of 15 December 1980 on entry, stay, settlement and removal of foreign nationals has recently been amended by the Law of 21 November 2017, which came into effect on 22 March 2018. Regarding the asylum procedure, the legislator has decided that, from now on, if the bodies responsible for examining the asylum application have good reasons to believe that the asylum seeker retains information that is nevertheless relevant at the stage of the application, they can invite him/her to produce this information, regardless the medium they are on. This is to be regarded as a new possibility for "digital search" of the asylum seeker, since his mobile phone, his computer, his data on social networks, etc. can thus be sieved. If the legislator bases this amendment on the consent of the person concerned, the validity of the consent of the asylum seeker appears relatively flawed in the light of the legislation on the protection of personal data, in particular the European Regulation on the protection of personal data, which entered into effect on May 25, 2018.

Le 22 juin 2017, le Gouvernement belge dépose, à l'initiative de son secrétaire d'État à l'asile et à la migration Monsieur T. Francken, un projet de loi tendant à modifier les lois du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers[2].

[1] Assistante à l'Université de Namur (CRIDS). Avocate au barreau du Brabant wallon. L'auteur remercie Elise Degrave pour ses conseils et sa relecture attentive.

[2] Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers, *Doc.*, Ch., 2016-2017, n° 2548/001.

Ce projet de loi a notamment pour but de transposer plusieurs directives européennes en matière d'asile et ayant pour vocation de mettre en place un régime d'asile commun, garantissant une « évaluation exhaustive et efficace des besoins de protection internationale des demandeurs d'asile ainsi qu'une égalité de traitement de ces demandeurs d'asile dans l'ensemble de l'Union »[3].

Le projet de loi adopté le 9 novembre 2017, est devenu loi du 21 novembre 2017. Cette loi a été publiée au *Moniteur belge* le 12 mars 2018 et est entrée en vigueur le 22 mars 2018.

Parmi les modifications législatives, on note des avancées positives visant à renforcer les garanties essentielles pour les demandeurs d'asile, comme le traitement par le Conseil du Contentieux des Étrangers (ci-après le « C.C.E. ») de tous les recours introduits à l'encontre d'une décision prise par le Commissariat général aux réfugiés et aux apatrides (ci-après le « C.G.R.A. »), la mise en place d'un schéma d'identification des personnes ayant des besoins procéduraux spéciaux ou encore l'interdiction de mesures d'éloignement forcé à l'encontre d'un demandeur de protection internationale lors du traitement de sa demande par le C.C.E. et le C.G.R.A.

Malheureusement, il apparaît que ces avancées sont contrebalancées par d'autres changements plus préoccupants pour les droits du demandeur d'asile, comme notamment le caractère non suspensif de certains recours, les délais raccourcis de certains de ceux-ci ainsi que la possibilité pour les instances compétentes de réaliser une fouille des supports qui sont en possession du demandeur d'asile pour obtenir des éléments leur permettant d'évaluer la demande de protection internationale.

S'agissant de cette dernière nouveauté, l'article 48/6, § 1er, alinéa 4, de la loi du 15 décembre 1980 autorise désormais les instances d'asile à solliciter, à certaines conditions, que leur soit remis tout support matériel ou immatériel en possession du demandeur afin de faciliter l'instruction de la demande et également vérifier son identité, son parcours…

Cette contribution a pour objectif d'analyser la portée de cet alinéa 4 du premier paragraphe de l'article 48/6 de la loi du 15 décembre 1980 et les implications qu'il emporte, au regard des droits et libertés du demandeur d'asile, et plus particulièrement son droit à la protection de ses données à caractère personnel.

I. HISTORIQUE DE LA RÉFORME ET DE L'ARTICLE 10 DU PROJET DE LOI

Le projet de loi initial a été déposé par le Gouvernement à l'aube des vacances d'été, le 22 juin 2017 et la Commission de l'intérieur a déposé son rapport sur le projet le 10 août 2017.

Le Haut-Commissariat des Nations Unies pour les réfugiés (ci-après le « HCR ») et la Commission de la Protection de la Vie Privée se sont prononcés en octobre 2017 sur ce projet de loi, texte qui comportait, en son article 10, la nouvelle mouture de l'article 48/6 de la loi du 15 décembre 1980.

Suite à ces avis, un amendement au texte de l'article 48/6 a été déposé en séance plénière de la Chambre le 19 octobre 2017, à l'initiative des députés fédéraux B. Hellings et W. De Vriendt[4].

[3] Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers, Exposé des motifs, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 5.

[4] Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres

Selon ces députés, s'appuyant sur les avis précités, l'article 10 du projet de loi est illégal en ce qu'il bafoue le principe du droit à protection de la vie privée des demandeurs d'asile, et devait être retiré du projet de loi.

Le texte a ensuite été renvoyé en commission pour analyse des différents avis.

Malgré la teneur des avis rendus sur le texte et des amendements proposés (l'opposition a en effet encore tenté d'amender le texte avant la dernière séance plénière), le texte est revenu de la commission tout à fait intact et a été adopté majorité contre opposition en séance plénière de la Chambre du 9 novembre 2017.

Les craintes de l'opposition ont été balayées par la majorité, le secrétaire d'État indiquant qu'il répondrait à celles-ci au travers d'un arrêté royal qui reprendrait les garanties à respecter dans le cadre de l'application de la nouvelle législation.

II. L'ARTICLE 48/6 DE LA LOI DU 15 DÉCEMBRE 1980

L'article 48/6 de la loi relative à l'accès au territoire, au séjour, à l'établissement et à l'éloignement des étrangers stipulait jusqu'alors que le demandeur d'asile, pour obtenir le statut de réfugié ou être reconnu comme « personne pouvant bénéficier de la protection subsidiaire » devait présenter, aussi rapidement que possible, « tous les éléments nécessaires pour étayer sa demande ».

La disposition prévoyait que si le demandeur d'asile ne parvenait pas à étayer certains aspects de ses déclarations par des preuves, il était jugé crédible, le bénéfice du doute lui étant accordé, à certaines conditions néanmoins.

L'article 10 du projet de loi tel qu'adopté le 9 novembre 2017 a modifié l'article 48/6 précité, dans lequel il insère notamment un paragraphe premier libellé comme suit : « Le demandeur d'une protection internationale doit présenter aussi rapidement que possible tous les éléments nécessaires pour étayer sa demande. Il appartient aux instances chargées de l'examen de la demande d'évaluer, en coopération avec le demandeur, les éléments pertinents de la demande de protection internationale. Les éléments visés à l'alinéa 1er correspondent notamment aux déclarations du demandeur et à tous les documents ou pièces en sa possession concernant son identité, son âge, son passé, y compris ceux des membres de la famille à prendre en compte, le ou les pays ainsi que le ou les lieux où il a résidé auparavant, ses demandes antérieures, ses itinéraires, ses titres de voyage, ainsi que les raisons justifiant sa demande de protection internationale.

L'absence des éléments visés à l'alinéa 1er, et plus particulièrement l'absence de preuve quant à l'identité ou la nationalité, qui sont des éléments centraux de la procédure d'évaluation d'une demande de protection internationale, constitue une indication défavorable concernant la crédibilité générale du récit du demandeur, à moins que le demandeur ne présente une explication satisfaisante à cette absence »[5].

Le nouveau texte de loi va donc un pas plus loin dans l'exigence, dans le chef du demandeur d'asile, de présenter les éléments étayant sa demande de protection, mais également dans la sanction attachée à un manque de transparence dans la communication de ces éléments, celui-ci étant considéré comme une brèche dans la crédibilité de son récit.

catégories d'étrangers, Amendement, *Doc.*, Ch., 2016-2017, n° 2548/010.

5 Projet de loi précité, *Doc.*, Ch., 2016-2017, n° 2548/001, pp. 236-237.

Mais ce n'est pas tout, puisque le texte de de loi poursuit en ces termes, en ajoutant un quatrième alinéa au paragraphe premier : « Si les instances chargées de l'examen de la demande ont de bonnes raisons de penser que le demandeur retient des informations, pièces, documents ou autres éléments essentiels à une évaluation correcte de la demande, elles peuvent l'inviter à produire ces éléments sans délai, quel que soit leur support. Le refus du demandeur de produire ces éléments sans explication satisfaisante pourra constituer un indice de son refus de se soumettre à son obligation de coopération visée à l'alinéa 1er »[6].

Il s'agit de la possibilité de fouille des supports qui sont en possession du demandeur d'asile, qui n'a pas manqué de faire débat avant l'adoption du texte.

In concreto, cette disposition permet aux instances chargées de l'instruction de la demande, à savoir le C.G.R.A. et l'instance d'appel, le C.C.E., d'inviter le demandeur à produire les éléments dont elles ont de bonnes raisons de penser qu'ils se trouvent en possession du demandeur, bien que ce dernier ne les a pas déclarés spontanément, ce malgré son obligation générale de coopération[7].

La communication de ces éléments peut se faire quel que soit le support sur lequel ils sont stockés, ce qui implique que le support puisse être de toute nature : matériel, immatériel, « en ce compris toute pièce, tout document, tout objet, tout appareil de communication (téléphone portable, tablette, ordinateur portable, …), tout compte de réseau social sur Internet (*Facebook*, *Twitter*…), tout support informatique (clé USB, CD-(ROM), carte mémoire, …) susceptible de contenir les éléments susvisés »[8].

Cette nouveauté est apparentée à une véritable « perquisition numérique » du demandeur d'asile, dans la mesure où son *smartphone*, son ordinateur, son compte *Facebook* … – et toutes les données qu'ils contiennent (liste de contacts, conversations, *e-mails*, photos, …) – pourront être passées au crible.

Or, il est évident que pour les demandeurs d'asile, ces supports sont souvent très précieux dans la mesure où ils permettent de conserver un lien avec leur famille et leur pays d'origine et qu'ils contiennent des morceaux de vie précieux qui les aident à surmonter la période difficile qu'ils traversent généralement.

Cette nouvelle disposition législative mérite donc d'être analysée, à l'aune des droits et libertés des demandeurs d'asile, et notamment du respect de leur vie privée.

A. Un corollaire : l'article 57/7 de la loi du 15 décembre 1980, nouvelle mouture

Notons que l'article 57/7 de la loi du 15 décembre 1980, toiletté lors de la réforme, légalise désormais une pratique apparemment déjà bien ancrée dans le chef du C.G.R.A., à savoir la consultation et l'utilisation, sans permission des demandeurs d'asile, de la partie publique (et donc non sécurisée) des profils de ceux-ci sur les réseaux sociaux comme *Facebook*[9].

Le § 2 de l'article 57/7 dispose en effet que : « le Commissaire général aux réfugiés et aux apatrides peut consulter et utiliser pour l'évaluation d'une demande de protection internationale des informations de toute nature

6 *Ibid.*, p. 237.

7 Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 34.

8 *Ibid.*, p. 36.

9 V. Henkinbrant, « D'une curieuse idée du consentement : une plongée sans fond dans la vie privée des demandeurs d'asile », Édito de l'ADDE, Newsletter n° 134, septembre 2017, disponible à l'adresse : http://www.adde.be/publications/newsletter-juridique.

envoyées ou reçues par voie électronique par le demandeur de protection internationale, qui n'ont pas été destinées personnellement au Commissaire général aux réfugiés et aux apatrides mais qui sont accessibles au public».

L'exposé des motifs du projet de loi nous apprend qu'en réalité, le profil *Facebook* n'est pas le seul visé, mais bien également des forums de discussion et d'Internet qui ne sont pas protégés ou sécurisés et qu'il s'agit généralement d'une recherche anticipative, avant l'entretien avec le demandeur d'asile, afin de pouvoir justement, lors de l'entretien, le questionner à propos des informations dénichées sur ces réseaux[10].

Jusqu'à présent, cette disposition est présentée par les travaux parlementaires comme conforme à la loi du 8 décembre 1992 relative à la protection de la vie privée, estimant que le traitement de données accessibles à tout public par le C.G.R.A. s'impose pour des «motifs importants d'intérêt public»[11].

Le législateur s'appuie sur des décisions rendues par le C.C.E., qui a jugé à plusieurs reprises que le C.G.R.A. pouvait utiliser les données publiques et accessibles d'un compte *Facebook* et que cela ne constituait pas une violation du droit à la vie privée, estimant qu'il appartenait au demandeur de masquer les informations qu'il ne voulait pas partager avec tout le monde[12].

Pour les données à caractère personnel qui ne sont pas exposées publiquement, l'exposé des motifs de l'article 57/7 de la loi renvoie à celui développé pour l'article 48/6, que nous exposerons ci-après.

10 Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 137.

11 *Ibid.*, p. 137.

12 C.C.E. n° 82 384 du 4 juin 2012; C.C.E. n° 116 470 du 3 janvier 2014; C.C.E. n° 141 224 du 8 janvier 2014 cités dans l'Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 138.

B. Les failles de l'article 48/6, § 1er, alinéa 4, de la loi du 15 décembre 1980

La possibilité de procéder à une perquisition numérique des supports en possession du demandeur d'asile est affectée de plusieurs failles, relevées par les partis d'opposition au cours du processus législatif, par la Commission de la protection de la vie privée et le H.C.R., et relayées dans les médias, en sorte qu'elles méritent une brève analyse.

1. Une ratio legis tronquée

Cette possibilité d'analyse des supports que le migrant possède est annoncée par le législateur comme permettant au C.G.R.A. de vérifier notamment la nationalité de celui-ci ou son pays d'origine.

Déjà en juin 2016, suite à une rencontre avec son homologue danois, Monsieur Francken avait émis l'idée de rendre légal le fait de fouiller dans les GSM et ordinateurs des migrants afin d'établir leur identité. À cette occasion, le secrétaire d'État avait avancé «qu'entre 60 et 70 %» des demandeurs d'asile mentent à propos d'un aspect de leur identité (nom, âge, trajet qu'ils ont suivi, pays d'origine…)[13].

L'opposition n'a toutefois pas souhaité se contenter de ces chiffres et a interpellé le secrétaire d'État sur ces chiffres considérés comme «fantaisistes», à plusieurs reprises durant le processus législatif ayant conduit à l'approbation de cet article[14].

13 «Théo Francken veut vérifier les GSM et ordinateurs des demandeurs d'asile», *Le Soir*, 29 juin 2016, disponible à l'adresse: http://plus.lesoir.be/48092/article/2016-06-29/theo-francken-veut-verifier-les-gsm-et-ordinateurs-des-demandeurs-dasile.

14 Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers, Rapport fait au nom de la Commission de l'intérieur, des affaires générales et de la fonction publique, *Doc.*, Ch., n° 2548/002, p. 19 et p. 32.

En effet, il a été avancé lors des débats en commission que selon certaines sources, dont FRONTEX, la fraude à la nationalité dans le chef des demandeurs d'asile ne concernait que 10 à 15 % des cas[15].

L'opposition n'a cessé de prôner le fait qu'« une mesure drastique comme la consultation d'un gsm ou d'une tablette, ainsi que le prévoit le projet de loi à l'examen, doit être fondée sur des chiffres conformes à la réalité et non sur de fausses statistiques »[16].

Trois questions avaient été posées au secrétaire d'État par un député de l'opposition au sujet de ces statistiques : le nombre de constats avérés de fraude à l'identité pour 2013, 2014, 2015 et les six premiers mois de 2016 (i), le nombre de cas avérés de fraude à l'identité rapporté au nombre de demandes d'asile introduites (ii), le top trois des nationalités pour lesquelles les fraudes sont le plus souvent constatées (iii)[17].

Le secrétaire d'État a répondu à ces questions en commençant par admettre que sa « déclaration selon laquelle 60 à 70 % des demandeurs d'asile ne disent pas toute la vérité durant la procédure d'asile est basée sur une estimation sommaire » et en indiquant que, dans bon nombre de dossiers, on pouvait tout simplement mettre en doute l'authenticité des déclarations dont la preuve concrète ne peut pas être apportée (ex. : itinéraires suivis d'écrits sommairement, récits relatés de manière similaire par plusieurs personnes, motif de l'asile exagéré, …)[18].

Il ressort de ce qui précède que la *ratio legis* du texte ne semble donc pas aussi solide que ce qui avait été initialement annoncé par le législateur.

Outre cette première faille, le texte de l'article 48/6, § 1er, alinéa 4, de la loi du 15 décembre 1980 pose d'autres problèmes au regard des droits et libertés des personnes demandeuses d'asile.

2. *Une fouille non encadrée – L'appréciation souveraine des « bonnes raisons »*

Comme indiqué ci-avant, le nouvel article 48/6, § 1er, alinéa 4, de la loi du 15 décembre 1980 prévoit désormais que : « si les instances chargées de l'examen de la demande *ont de bonnes raisons de penser que*[19] le demandeur retient des informations, pièces, documents ou autres éléments essentiels à une évaluation correcte de la demande, elles peuvent l'inviter à produire ces éléments sans délai, quel que soit leur support (…) ».

Cela signifie que ce sont les instances d'asile, à savoir le C.G.R.A. ou le C.C.E., qui pourront évaluer si le recours à la fouille numérique se justifie.

Les termes « bonnes raisons »

À juste titre, certains parlementaires ont interrogé le secrétaire d'État sur ce qu'il convenait d'entendre par les termes « bonnes raisons »[20].

Ce dernier s'est contenté de renvoyer à l'exposé des motifs de la loi, considérant que celui-ci répondait à la question et déterminait la manière d'évaluer le caractère satisfaisant ou non de l'explication donnée par le deman-

15 Rapport fait au nom de la Commission de l'intérieur, des affaires générales et de la fonction publique précité, *Doc.*, Ch., n° 2548/002, p. 19 et p. 32.

16 Rapport fait au nom de la Commission de l'intérieur, des affaires générales et de la fonction publique précité, *Doc.*, Ch., n° 2548/002, p. 51.

17 Q&R, *Doc.*, Ch., n° QRVA 54083, Question n° 748 de Monsieur le député Benoit Hellings au secrétaire d'État, 2015-2016, p. 419.

18 *Ibid.*, p. 420.

19 Souligné par nous.

20 Rapport fait au nom de la Commission de l'intérieur, des affaires générales et de la fonction publique précité, *Doc.*, Ch., n° 2548/002, p. 54.

deur pour justifier le refus ou l'impossibilité de communiquer les informations demandées.

Si l'on se penche sur l'exposé des motifs de la loi, celui-ci fournit effectivement une liste non exhaustive de ce qui pourrait constituer des indices de rétention d'informations par le demandeur d'asile, à savoir « des déclarations lacunaires (imprécises, incohérentes, inconsistantes, contradictoires, et/ou invraisemblables, etc.) (…) sur des points importants de sa demande ; la présence d'incohérences ou de contradictions entre les déclarations du demandeur et d'autres informations disponibles par ailleurs » ou encore « le fait que le demandeur présente un profil tel qu'il pourrait être amené à vouloir minimiser ou au contraire amplifier certains aspects de son vécu, ayant un impact sur l'évaluation de la réalité de la crainte et des problèmes qu'il pourrait rencontrer en cas de retour, de même que sur l'application éventuelle de causes de retrait, de cessation, voire d'exclusion des statuts de protection internationale etc. »[21].

Dans de telles circonstances ainsi que face à d'autres situations non listées mais similaires, le C.G.R.A. et le C.C.E. peuvent donc fouiller les documents et les supports en possession du demandeur, y compris son gsm ou ordinateur, « sans que cela ne doive donner lieu à une motivation particulière à son égard »[22].

Ce procédé – couramment appelé « perquisition numérique » – et celui pratiqué lors de véritables perquisitions d'outils numériques en matière pénale ne résistent pas à un examen sérieux de la comparaison.

La perquisition en matière pénale

La saisie pénale est définie par la Cour de cassation comme une « mesure conservatoire par laquelle l'autorité compétente, selon la loi et à propos d'une infraction, soustrait une chose à la libre disposition de son propriétaire ou de son possesseur et, en vue de la manifestation de la vérité, de la confiscation, de la restitution ou de la sécurité des intérêts civils, et la place sous elle »[23].

L'article 39*bis* du Code d'instruction criminelle (ci-après le « C.i.cr. ») traite spécifiquement la question de la recherche dans un système informatique saisi (ou une partie de celui-ci) et prévoit en son deuxième paragraphe que cette recherche peut être décidée par un officier de police judiciaire, sans préjudice du procureur du Roi, qui peut également ordonner ce type de recherche.

Cette recherche peut uniquement s'étendre aux données sauvegardées dans le système informatique qui est soit saisi, soit susceptible d'être saisi, et non aux liaisons externes du système informatique (article 39*bis*, § 2, C.i.cr.).

Par contre, s'agissant de l'interception, la prise de connaissance, l'exploration et l'enregistrement des communications privées ou des données d'un système informatique à l'aide de moyens techniques, seul le juge d'instruction peut ordonner ces méthodes de recherche (article 90*ter* C.i.cr.).

Lorsqu'un officier de police contrôle le contenu d'un *smartphone* saisi ou, de manière générale, qu'une lecture de système informatique est autorisée par un juge d'instruction, ces procédés sont encadrés et ne sont permis que dans des circonstances spécifiques, si des garanties sont prévues.

En matière d'asile, ces recherches et contrôles semblent au contraire autorisés sans garanties particulières, et hors du cadre d'une recherche relative à la commission d'une infraction.

21 Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, pp. 34-35.

22 *Ibid.*, p. 34.

23 Cass., 25 février 2003, *Pas.*, 2003, p. 412.

Le statut des instances d'asile

On peut également s'étonner du fait que le C.G.R.A., instance administrative, soit, dans les faits, dotée du même pouvoir d'examen qu'un officier de police, un représentant du ministère public ou un magistrat.

L'exposé des motifs de l'article 48/6, § 1er, alinéa 4, de la loi du 15 décembre 1980 prévoit en outre que bien que ce soit le C.G.R.A. qui soit l'instance dotée de pouvoirs d'instruction, le C.C.E. peut également « se faire remettre par les parties toutes les pièces et informations concernant les affaires sur lesquelles il doit se prononcer », ce sur base de l'article 39/62 de la loi du 15 décembre 1980, demeuré inchangé[24].

Les travaux préparatoires de cet article 39/62, cités dans l'exposé des motifs de l'article 48/6, § 1er, alinéa 4, disposent que : « le fait que le Conseil du Contentieux des Étrangers ne dispose pas d'une compétence d'instruction ne signifie pas que le Conseil devrait subir passivement l'instance (…), de plus il ne peut pas être exclu que certaines informations ou documents fassent défaut alors que ceux-ci sont indispensables pour la solution du litige. Si tel est le cas, le Conseil peut recueillir ces informations par un échange direct de courriers avec les parties »[25].

Il ressort de ce qui précède que tant le C.G.R.A. que le C.C.E. disposent à présent d'un véritable pouvoir de contrôle et d'examen des supports numériques du demandeur d'asile, ce en vertu de la loi du 15 décembre 1980. Or, au contraire de la loi pénale, la loi du 15 décembre 1980 n'édicte aucune garantie par rapport aux droits fondamentaux du demandeur d'asile, et notamment face à l'importante ingérence dans sa vie privée qu'engendre la fouille numérique comme mesure d'instruction d'une demande.

Au contraire, la définition des « bonnes raisons » reprise dans l'exposé des motifs de la loi est relativement large. Les instances d'asile disposent dès lors d'un pouvoir d'appréciation étendu qui risque, face au récit d'un demandeur d'asile, de les amener à prendre connaissance de ses données, de manière tout à fait arbitraire à défaut de balises suffisamment précises pour encadrer de telles actions, et sans devoir motiver leur décision.

Ce constat ne manque pas de révéler une seconde faille de l'article 48/6, § 1er, alinéa 4, de la loi du 15 décembre 1980, s'agissant du respect des droits fondamentaux du demandeur d'asile.

3. *Des données à caractère personnel traitées illégalement*

Si l'article 57/7 de la loi du 15 décembre 1980 légalise la fouille des données laissées accessibles au public par les demandeurs d'asile, l'article 48/6, § 1er, alinéa 4, de la loi traite lui aussi des données publiques éventuellement accessibles sur les supports du demandeur d'asile (ex. partie publique du profil Facebook). Mais ce nouvel article va plus loin, puisqu'il est relatif en plus aux données à caractère personnel (ex. photos du *smartphone*, messages, e-mails, partie privée du profil et amis Facebook, liste d'appels, destinations du GPS…).

Cette fouille constitue un traitement de données à caractère personnel du demandeur d'asile, à savoir celles concernant son identité et sa vie privée, au sens du Règlement général sur la protection des données (ci-après, « le R.G.P.D. » ou « le Règlement »), applicable depuis le 25 mai 2018 et définissant le traitement comme : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration,

[24] Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 34.

[25] *Ibid.*, p. 34.

la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction[26].

Il s'agit d'une définition similaire à celle présente dans la loi du 8 décembre 1992[27], qui vient de céder le pas au R.G.P.D.

Dès la rédaction du projet de loi, la question du droit au respect de la vie privée et de la protection des données à caractère personnel du demandeur d'asile n'a pas manqué de faire réagir les parlementaires de l'opposition.

L'exposé des motifs de l'article 48/6, § 1er, alinéa 4, de la loi se contente en effet d'indiquer que « cet alinéa est conforme à la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992 », dans la mesure où, en entamant une démarche délibérée consistant en une demande de protection internationale, le demandeur se soumet à des obligations de coopération.

Comme les sollicitations des instances d'asile visent à évaluer la demande et le besoin de protection dans le chef du demandeur d'asile, le législateur estime que l'accès, la récole et le traitement de ses données à caractère à personnel se font donc, pour le demandeur d'asile, de manière tout à fait consentie.

L'exposé des motifs dispose en effet que : « l'accès, la récolte et le traitement de ces informations à caractère privé se font donc de manière consentie et participent, de manière loyale et légitime, à l'établissement de faits nécessaires à l'exercice de la mission poursuivie par les instances chargées de l'examen de la demande »[28].

D'après le législateur, cette disposition suffit pour donner un fondement légal au traitement de données des demandeurs d'asile, à savoir le consentement.

Non satisfaite de cette explication, l'opposition a émis des préoccupations à propos du bon respect, par le législateur, de ce droit à la protection de la vie privée[29].

Le secrétaire d'État s'est contenté de répondre en indiquant que ces contrôles des gsm et autres équipements informatiques existaient déjà avant, qu'il ne s'agissait dès lors pas d'une nouvelle compétence qui était attribuée au C.G.R.A., mais uniquement d'une manière d'opérer la distinction avec les mesures existant dans certains pays comme la Norvège ou le Danemark, où les services de police ont la possibilité d'imposer, sous le contrôle du Parquet, l'examen de ce matériel dès l'enregistrement de la demande d'asile[30].

Il convient toutefois d'examiner la teneur de ce consentement, tel que prévu par la législation en matière de protection des données, et de confronter les principes à l'application, par les instances d'asile, de la possibilité que leur offre le nouvel article 48/6, § 1er, alinéa 4.

26 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, 4 mai 2016, article 4.2).

27 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, article 1er, § 2.

28 Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 37.

29 Rapport fait au nom de la Commission de l'intérieur, des affaires générales et de la fonction publique précité, *Doc.*, Ch., n° 2548/002, p. 19, p. 32, p. 33 et p. 51.

30 *Ibid.*, p. 96.

C. Le consentement comme justification du traitement des données à caractère personnel du demandeur d'asile

On l'a dit, le législateur s'est retranché derrière le consentement qui serait prétendument donné par le demandeur d'asile pour justifier la nouvelle mesure édictée à l'article 48/6, § 1er, alinéa 4, de la loi.

1. La définition de la notion de consentement

L'article 1er, § 8, de la loi du 8 décembre 1992 de la loi relative à la protection de la vie privée définit la notion de «consentement de la personne concernée» comme «toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement».

L'article 4, 11), du R.G.P.D. définit quant à lui le consentement comme «toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que les données à caractère personnel la concernant fassent l'objet d'un traitement».

L'article 6 du R.G.P.D., qui énumère les différentes bases légales sur lesquelles peut reposer un traitement, dispose que le traitement pourra notamment être licite si «la personne a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques»[31].

Ce consentement, pour légitimer le traitement de données, devra également remplir certains critères légalement définis, et récemment commentés par le Groupe 29 au travers de *guidelines*.

2. Les contours de la notion de consentement dans le R.G.P.D. et la teneur du consentement des demandeurs d'asile

i. Le consentement doit être exprimé librement

L'exigence du caractère *libre* du consentement signifie que la personne concernée doit avoir été en mesure de réellement faire un choix, s'agissant du traitement de ses données à caractère personnel. Le consentement ne sera pas considéré comme ayant été *librement donné* si la personne concernée n'a pas réellement choisi de le donner, si elle s'est sentie obligée de consentir au traitement ou si elle a été confrontée à un risque de subir des conséquences négatives en cas de refus de donner son consentement[32].

Lorsque le responsable de traitement est une autorité publique, le Groupe 29 émet des réserves quant au fait que le consentement puisse être donné librement par la personne concernée et dès lors, que ce consentement puisse, à lui seul, légitimer le traitement[33].

En effet, il est probable que, dans pareil cas, il existe un déséquilibre de forces entre le responsable de traitement et la personne concernée, en sorte que cette dernière n'aurait pas véritablement d'autre(s) alternative(s) que de donner son consentement audit traitement.

D'autres bases légales pourraient dans ce cas justifier de manière plus appropriée que les autorités publiques réalisent un traitement de données, comme par exemple si le traitement est «nécessaire au respect d'une obligation légale à laquelle le responsable du traitement

31 Règlement européen relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données, précité, article 6.1.a).

32 Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 6.

33 Règlement européen relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données, précité, considérant 43.

est soumis » ou si le traitement est « nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique »[34].

En réalité, le déséquilibre de forces n'est pas limité aux relations entre une autorité publique et la personne concernée, mais caractérise toute situation dans laquelle cette personne ne peut exercer librement son choix de consentir au traitement, parce que le refus de consentir présente un risque, est soumis à une forme de pression, d'intimidation, de coercition ou entraîne des conséquences néfastes pour la personne concernée[35].

Le considérant n° 42 du R.G.P.D. édicte en outre que : « le consentement ne devrait pas être considéré comme ayant été donné librement si la personne ne dispose pas d'une véritable liberté de choix *ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ».

Cela signifie que le responsable de traitement, en plus d'être contraint de solliciter le consentement de la personne concernée en veillant à ne pas se placer dans un rapport de forces, doit être en mesure de démontrer que si la personne concernée refuse ou retire son consentement, elle n'en subira aucun préjudice, aucun désavantage ou aucune conséquence néfaste.

En pratique, s'agissant de la fouille numérique du demandeur d'asile, on peut douter du caractère libre que présentera le consentement du demandeur d'asile confronté à une administration qui lui demandera de présenter son *smartphone*, par exemple.

Comme énoncé, le simple fait que le demandeur d'asile se trouve face à une autorité le place dans une situation d'infériorité, jugée comme rendant l'expression du consentement systématiquement colorée d'un rapport de forces, et donc tronquée.

Deuxièmement, la pression qui pèse sur le demandeur d'asile est manifeste puisque l'article 48/6, § 1er, alinéa 4, de la loi dispose que si celui-ci refuse de donner accès aux supports qu'il détient, ce sans explications satisfaisantes, ce refus pourra être considéré comme « un indice de son refus de se soumettre à son obligation de coopération ».

L'exposé des motifs de la loi n'hésite pas, en plus, à reconnaître que les explications qui pourraient être avancées par le demandeur d'asile pour justifier son refus de consentir à la fourniture de ses données seront rarement jugées satisfaisantes, vu l'importance des éléments recherchés et l'exigence d'une explication étayée et circonstanciée[36].

Il semble donc que le demandeur d'asile n'aura en réalité pas le choix que de fournir les informations personnelles dont il dispose, dans la mesure où s'il refuse, il s'agira d'un manquement à son obligation de coopération et donc d'un élément négatif dans l'examen de sa demande.

La pression sera donc immense, au vu des conséquences négatives d'un refus sur l'issue de sa demande d'asile.

Il convient aussi de noter que la transmission des supports d'informations devra intervenir *sans délai*, en sorte que le demandeur n'aura pas le temps de réfléchir avant de donner, ou non, son consentement.

Le 11 octobre 2017, la Commission de la protection de la vie privée a rendu un avis d'initiative sur le projet de loi, dans lequel elle

34 *Ibid.*, articles 6.1 c) et 6.1 e).

35 Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 8.

36 Exposé des motifs précité, *Doc.*, Ch., 2016-2017, n° 2548/001, p. 36.

s'est notamment penchée sur l'article qui nous occupe[37].

Par cet avis, la Commission de la vie privée a commencé par s'étonner du fait que le secrétaire d'État ne l'avait absolument pas consultée au sujet du projet de loi, ce contrairement à ce que prescrit la directive 95/46/CE[38].

La Commission n'a pas manqué de soulever que, depuis l'entrée en vigueur du R.G.P.D. (en mai 2016), un avis devait lui être demandé s'agissant des traitements de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Or, la Commission a considéré que le traitement de données envisagé par le projet de loi (contrôle du *smartphone*, des profils sur les réseaux sociaux ou d'autres supports d'informations numériques) est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, en sorte que si on suit le R.G.P.D., un avis aurait dû être demandé à la Commission[39].

S'agissant du consentement du demandeur d'asile au traitement de ses données personnelles, la Commission a spécifiquement soulevé que: «La personne concernée se trouve donc dans une situation de soumission où la demande du collaborateur du C.G.R.A. d'accéder au smartphone ou aux informations privées de la page Facebook du demandeur d'asile sera rapidement considérée par ce dernier comme une injonction ou une obligation»[40].

La Commission a relevé qu'il manquait un cadre légal suffisant concernant la manière dont l'accès au support numérique est réalisé et d'autre part les droits de la personne concernée.

Le caractère libre du consentement qui pourrait éventuellement être exprimé est donc loin d'être garanti.

ii. Le consentement doit être spécifique

Lorsqu'un responsable de traitement collecte des données à caractère personnel, il doit le faire pour répondre à des finalités déterminées, explicites et légitimes, et il sera contraint de veiller à ce que les données soient traitées d'une manière compatible avec lesdites finalités[41].

Lorsque le traitement est basé sur le consentement de la personne concernée, celle-ci doit avoir consenti au traitement pour les finalités spécifiques déterminées au moment de la collecte de données.

Il s'ensuit que le consentement, pour être valablement donné, doit porter sur l'ensemble des finalités avancées par le responsable de traitement, et uniquement pour les activités spécifiques répondant à ces finalités[42].

Tant que les opérations de traitement répondent aux finalités auxquelles la personne concernée a consenti, le responsable de traitement agira en toute légalité.

37 Commission de la protection de la vie privée, avis n° 57/2017 du 11 octobre 2017.

38 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des données personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, article 28, alinéa 2.

39 Règlement européen relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données, précité, articles 57, alinéa 1er, 36, alinéa 2 et 35.

40 Commission de la protection de la vie privée, avis n° 57/2017, précité, p. 8.

41 Règlement européen relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données, précité, article 5.1.b).

42 Règlement européen relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données, précité, article 6.1.a) et considérant 32.

Par contre, si la personne concernée a consenti à une opération de traitement en particulier, le responsable de traitement ne pourra pas élargir le traitement à d'autres opérations répondant à d'autres finalités sur base de ce consentement, et devra veiller à obtenir un consentement de la personne pour chaque nouvelle finalité envisagée.

À chaque finalité de traitement doit correspondre une expression du consentement différente, formulée librement, pour répondre à la notion de consentement *libre et spécifique*.

On peut en l'espèce douter de ce que les instances d'asile, lors d'un entretien, prennent le temps d'expliquer au demandeur d'asile les finalités exactes pour lesquelles elles ont besoin d'accéder à ses données à caractère personnel, et encore moins que celui-ci consente, *in fine*, à l'une ou l'autre finalité de traitement éventuellement annoncée.

Seule l'assistance d'un avocat compétent en matière de protection des données lors de l'entretien pourrait le cas échéant pallier cette carence d'informations quant aux finalités du traitement de données.

iii. Le consentement doit être éclairé

L'exigence d'un consentement *éclairé* dans le chef de la personne concernée est un corollaire du principe de transparence qui gouverne, entre autres, la collecte et le traitement de données à caractère personnel.

Pour que le consentement soit éclairé, le Groupe 29 est d'avis que différentes informations doivent, au minimum, être fournies à l'individu[43] :

- l'identité du responsable de traitement ;
- la/les finalité(s) de traitement pour la/lesquelle(s) le consentement est requis ;
- le type de données qui va être collecté ;
- l'existence d'un droit, pour cet individu, de retirer son consentement à tout moment ;
- l'information à propos de l'utilisation des données pour des décisions fondées sur un traitement automatisé, y compris le profilage, conformément à l'article 22.2 du Règlement ;
- si le consentement est relatif à des transferts de données, sur les risques de transfert dans un pays tiers qui ne présenterait pas des garanties adéquates et suffisantes.

S'agissant de la forme que doit prendre la communication de ces informations, elle peut être diverse (écrite, orale, audio, vidéo, …) pour autant que le message soit facilement compréhensible pour toute personne, c'est-à-dire qu'elle ne peut consister en des clauses longues et inintelligibles ou rédigées en termes juridiques.

Le responsable de traitement doit veiller à ce que le consentement de la personne concernée soit donné sur base d'informations qui permettent à celle-ci de savoir exactement à quoi elles consentent[44].

De cette manière, le responsable de traitement garantit que l'individu a donné son consentement librement, pour les finalités spécifiques qu'il a exposées, et de manière éclairée, et en connaissant exactement la portée de son acceptation.

À nouveau, en pratique, on imagine mal comment la transmission de ces informations pourra se faire de manière détaillée et compréhensible pour le demandeur d'asile, lors d'un entretien.

[43] Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 13.

[44] Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 14.

La Représentation régionale du H.C.R. qui a été invitée à soumettre des commentaires sur le projet de loi, a fait savoir, au travers ses commentaires sur le texte, que l'exigence du consentement du demandeur était nécessaire pour le protéger, notamment au regard du droit à la dignité humaine et du droit à la vie privée[45].

Si le H.C.R. est d'avis que, dans certaines situations, la fouille ou la saisie des appareils électroniques des demandeurs de protection internationale peuvent se justifier, il faut respecter certaines conditions : « Étant donné le caractère intrusif de telles mesures, des garanties juridiques protégeant contre les saisies et fouilles abusives ne peuvent être restreintes ou refusées aux demandeurs »[46].

Le H.C.R. estime que ces fouilles ne pourront être pratiquées que pour poursuivre un but légitime, prévu par la loi et être nécessaires et proportionnées audit but, tout en étant basées sur un consentement libre et éclairé de la personne concernée.

Aucune autre précision n'est formulée par le H.C.R. sur la manière d'envisager la récolte de ce consentement, excepté que « la personne doit recevoir, sans délai, des informations adéquates concernant la procédure, ses buts et avoir accès à un avocat »[47], ce pour que la procédure soit parfaitement comprise et le consentement tout à fait éclairé lorsque le demandeur, éventuellement assisté de son avocat, donne accès à ses données.

iv. Le consentement ne peut être équivoque

Le considérant n° 32 du R.G.P.D. indique également que le consentement doit être donné par le biais d'un acte positif clair, qui peut être une déclaration écrite (y compris par voie électronique), une déclaration orale (enregistrée) ou se manifester par un autre comportement pour autant que l'acceptation de la personne concernée apparaisse clairement.

Enfin, ledit considérant prévoit qu'il « ne saurait dès lors y avoir consentement en cas de silence, de cases cochées par défaut ou d'inactivité » en sorte qu'on peut considérer qu'un acte clair consiste en une *action délibérée* par laquelle le sujet consent au traitement spécifié.

Cette action délibérée peut prendre différentes formes selon que le consentement est, ou non, exprimé par voie électronique ou de manière écrite.

Le Groupe 29 considère qu'un acte positif clair peut se manifester par des mouvements physiques (un *swipe* sur un écran, un signe devant une caméra, une inclinaison du *smartphone*) à condition que ces mouvements manifestent clairement un accord de la personne concernée[48].

À nouveau, la question de savoir, en pratique, quel acte positif clair sera considéré comme une manifestation de son consentement par le demandeur d'asile reste également entièrement ouverte et n'est, à ce jour, pas prise en compte par le législateur.

v. Le traitement des données sensibles requiert un consentement explicite

L'article 9 du R.G.P.D. traite des données sensibles, comme les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, les données concernant la santé et la vie sexuelle[49],

45 Projet de loi précité, *Doc.*, Ch., 2016-2017, n° 2548/004, Avis du Haut-Commissariat des Nations Unies pour les réfugiés (HCR), 4 octobre 2017, p. 7.

46 *Ibid.*, n° 14.

47 *Ibid.*, n° 15.

48 Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 17.

49 Liste non exhaustive des données sensibles reprises à l'article 9.1 du Règlement.

et dispose que le traitement de celles-ci est interdit, sauf dans certains cas, et notamment si la personne a donné son consentement *explicite* au traitement de ces données pour une ou plusieurs finalités spécifiques[50].

Le R.G.P.D., qui va déjà plus loin que la directive 95/46/CE en imposant l'expression d'un acte positif clair dans le chef de la personne qui consent au traitement de ses données, exige encore un effort supplémentaire de la part du responsable s'agissant du consentement au traitement de données sensibles puisque l'accord qui doit être donné doit être explicite.

Le Groupe 29 propose plusieurs pistes qui peuvent être considérées comme la manifestation, par l'individu, de son consentement explicite. Il peut s'agir soit une déclaration écrite confirmant expressément son accord sur le traitement, une déclaration écrite signée, ou, dans le contexte numérique un formulaire électronique à remplir, un *e-mail* à envoyer, un document signé à scanner et à envoyer au responsable, l'utilisation de la signature électronique ou même un consentement donné de manière orale, bien qu'il sera difficile à démontrer pour le responsable de traitement[51].

Une autre piste pourrait également consister en un processus de « double vérification », par lequel lorsque le responsable a expliqué à la personne concernée le traitement envisagé et les finalités visées et que cette dernière consent au traitement, le responsable lui demande de confirmer à nouveau cela dans un *e-mail* ou lui envoie un lien par *e-mail* qu'elle doit vérifier, ou lui envoie un SMS avec un code de vérification, cela pour confirmer sa volonté de consentir au traitement[52].

Il est évident que les supports numériques des demandeurs d'asile contiendront des données sensibles, lorsqu'on songe aux photos présentes sur son *smartphone*, à ses échanges d'e-mails, de messages, qui pourraient contenir des données sur son origine, ses opinions politiques, ses préférences sexuelles, …

Il conviendrait donc que les instances d'asile veillent à ce que le consentement qui est éventuellement donné soit d'autant plus « fort » et exprimé de manière parfaitement claire mais à nouveau, il est difficilement imaginable que tout cela soit scrupuleusement respecté en pratique.

vi. L'obtention du consentement doit être démontrée

L'article 7.1. du R.G.P.D. impose désormais au responsable de traitement, lorsqu'il base le traitement sur le consentement de la personne concernée, de démontrer que ce consentement a été recueilli.

La charge de la preuve incombe donc au responsable, qui est libre de développer les méthodes qu'il souhaite pour démontrer que le consentement a été recueilli légalement, en veillant à ce que ces méthodes n'engendrent pas de traitements complémentaires excessifs[53].

Si le R.G.P.D. ne définit pas la manière dont le responsable peut apporter cette preuve, le Groupe 29 considère que cette obligation vise à pouvoir démontrer, dans chaque cas particulier, que le consentement a été valablement recueilli et ce, tout au long du processus de traitement.

S'agissant de la durée pour laquelle un consentement est donné, le Groupe 29 recommande

50 Règlement européen relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données, précité, article 9.2.a).

51 Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, pp. 18-19.

52 *Ibid.*, p. 19.

53 *Ibid.*, p. 20.

aux responsables de veiller, à intervalles réguliers, à redemander à la personne concernée de consentir à nouveau au traitement, de manière à s'assurer qu'elle reste parfaitement informée sur la manière dont ses données sont traitées et dans quel but[54].

Aucune méthode de preuve d'obtention de ce consentement n'est actuellement envisagée par la loi s'agissant de la fouille numérique et il est, comme pour toutes les autres exigences que doit recueillir un traitement basé sur le consentement, permis de douter sur la méthode qui va être effectivement appliquée dans les prochains mois pour prouver que le consentement a bien été obtenu, ce alors qu'il sera probablement exprimé oralement, lors d'un entretien relativement bref.

vii. Le consentement peut être retiré à tout moment

L'article 7.3 du R.G.P.D. prévoit que la personne concernée peut, à tout moment, retirer son consentement à ce que ses données soient traitées.

Le Groupe 29 a insisté sur le fait que ce retrait devait être *facile* et possible de la même manière que par laquelle la personne concernée donne son consentement, sans engendrer aucun inconvénient[55].

Si la procédure de retrait ne respecte pas les exigences prévues par le Règlement, l'ensemble du mécanisme basé sur le consentement de l'individu n'est pas conforme audit Règlement.

La personne concernée doit évidemment être informée de l'existence de ce droit de retrait, et sur la manière de l'exercer.

Si le consentement est retiré par l'individu, les opérations de traitement antérieures à ce retrait seront toujours légales, pour autant bien entendu qu'elles aient été réalisées en respectant le Règlement.

viii. Considérations finales en matière de consentement

De manière générale, on constate que la nouvelle législation européenne sur la protection des données a renforcé l'exigence, pour le responsable de traitement, d'obtenir le consentement de la personne concernée en respectant des conditions strictes.

Le législateur européen a ainsi voulu réagir aux situations multiples dans lesquelles un consentement de mauvaise qualité servait de fondement au traitement des données, et insisté sur le fait que le consentement devait être de qualité et exprimé dans un contexte tel que la personne concernée soit complètement autonome[56].

Le responsable de traitement devrait donc soit s'appuyer sur un consentement de bonne qualité si celui-ci constitue le fondement du traitement, soit utiliser une autre base légitimant ce traitement des données, étant toutefois précisé que la base de traitement ne peut être modifiée en cours de processus[57].

Il est toutefois permis de s'interroger, en pratique, sur la manière dont va être recueilli ce consentement, dont les exigences légales ont été examinées *supra*, à la lumière de l'entrée en vigueur du R.G.P.D. et du déroulement d'un entretien avec un agent d'une instance d'asile.

54 *Ibid.*, p. 20.
55 *Ibid.*, p. 21.
56 C. de Terwangne, K. Rosier, B. Losdyck, « Le Règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *J.D.E.*, 2017, p. 306.
57 Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 22.

Quel acte positif clair le demandeur d'asile va-t-il devoir fournir pour démontrer son consentement ? De quelle manière les instances d'asile seront-elles en mesure de démontrer que le consentement a été recueilli ? De quelle manière le demandeur d'asile va-t-il être informé du traitement envisagé et des finalités de celui-ci ? Sera-t-il informé qu'il peut retirer à tout moment son consentement à ce que ses données soient collectées et traitées ?

Enfin, d'un point de vue pratique, les situations dans lesquelles le demandeur d'asile ne parle pas les langues nationales et ne comprend pas ce qui lui est demandé ne sont pas rares, et il est dès lors difficilement imaginable que celui-ci, non assisté d'un avocat, intègre complètement les informations légales qui lui seraient données au sujet du processus de traitement de ses données ainsi que les enjeux de ce traitement, si de telles informations devaient lui être fournies.

Autant d'interrogations et de préoccupations sur lesquelles le législateur n'a pas jugé utile de se pencher jusqu'à présent.

Or, il est évident que le traitement de données envisagé ne sera pas légalement effectué, ce qu'avaient déjà relevé la Commission de la protection de la vie privée et le Haut-Commissariat des Nations Unies avant l'adoption du texte.

Le H.C.R. avait en plus indiqué qu'il était souhaitable que la loi prescrive explicitement que le consentement éclairé du demandeur pour la production d'éléments estimé essentiels par l'instance pour évaluer sa demande doit être demandé, estimant que la facilité d'accès aux données contenues dans les appareils de communication n'autorisait pas des fouilles systématiques et non justifiées[58].

Malgré cette recommandation, la loi ne reprend pas, de manière explicite, l'exigence de recueillir le consentement du demandeur avant d'explorer ses supports mais se contente d'indiquer que les instances d'asile doivent *l'inviter* à produire ces éléments et que, si ce dernier émet un *refus*, cela affaiblira son dossier.

On le voit, il n'a même pas été envisagé de prévoir clairement dans le texte de loi la base première du traitement, à savoir le principe de l'obtention du consentement…

III. CONCLUSION

La nouvelle possibilité de fouille des supports numériques du demandeur d'asile est critiquable, tant sur son fondement, que sur les implications qu'elle emporte pour la protection des données à caractère personnel de cette personne.

Celle-ci, souvent démunie lorsqu'elle se trouve confrontée à un agent d'une instance d'asile, serait en effet, d'après le législateur, apte à donner son consentement au traitement de ses données à caractère personnel, ce qui garantirait que les instances agissent en toute légalité.

En réalité, il n'en est rien et il est même plutôt improbable que le demandeur d'asile ait véritablement la latitude d'exprimer s'il consent ou non à l'examen de ses supports comme son gsm, sa tablette ou son ordinateur et des données qu'ils contiennent.

Comme l'a relevé l'opposition au stade du projet de loi, mais également la Commission de la protection de la vie privée et le Haut-Commissariat des Nations Unies, cette fouille numérique devait être encadrée par des garanties nécessaires pour protéger les droits et libertés des migrants.

[58] Projet de loi précité, *Doc.*, Ch., 2016-2017, n° 2548/004, Avis du Haut-Commissariat des Nations Unies pour les réfugiés (HCR), 4 octobre 2017, n° 15.

Malgré ces avis, l'article a été adopté sans modifications, le secrétaire d'État précisant que les garanties entourant cette possibilité de fouille numérique seraient précisées ultérieurement au travers d'un arrêté royal…

Le législateur, en modifiant l'article 48/6 de la loi du 15 décembre 1980, s'est en effet contenté d'avancer que son texte était légal, compte tenu des obligations de coopération auxquelles le demandeur d'asile se soumettait en introduisant une demande de protection internationale, celui-ci consentant par ce fait à ce qu'on instruise sa demande, par quelque manière que ce soit.

On peut se demander pourquoi le législateur n'a pas basé l'accès et le traitement des données du demandeur d'asile sur un autre fondement juridique, comme éventuellement la bonne exécution d'une mission d'intérêt public ou un motif important d'intérêt public (qui est d'ailleurs le fondement légal utilisé pour légitimer la consultation des données publiques du demandeur) plutôt que sur le consentement de la personne concernée, qui se révèle aussi tronqué que bancal, s'agissant des conditions légales qu'il doit requérir.

Avec l'entrée en vigueur du R.G.P.D., il est évident que ce fondement légal ne pourra plus être modifié, étant donné que le Groupe 29 a expressément prévu que le responsable de traitement ne pouvait pas, au gré de sa volonté et des circonstances de l'espèce, modifier la base légale de son traitement[59].

Reste dès lors à voir si cet article de loi sera entouré de garanties nécessaires au respect des droits et libertés du demandeur d'asile, comme la protection de ses données à caractère personnel, ou si seul un recours en annulation contre celui-ci permettra de protéger lesdites données de toute intrusion.

À l'heure actuelle, ni la loi telle que modifiée, ni aucun autre acte législatif ou exécutif ne prévoient ces garanties.

En l'attente, le demandeur d'asile non assisté n'a véritablement d'autre choix que de confier son *smartphone* ou son ordinateur aux instances d'asile, qui pourront à leur gré examiner toutes les données personnelles contenues sur ces supports, souvent très précieux et symboles de liens avec une famille ou un pays lorsqu'on se trouve sur la route de l'exil.

[59] Article 29 Data protection working party, Guidelines on Consent under Regulation 2016/679, 28 novembre 2017, WP259, p. 22.