COMMISSION
EUROPÉENNE

Bruxelles, le 29.2.2016
COM(2016) 93 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

La disponibilité et le degré de maturité de la technologie permettant d'identifier une personne sur la base des empreintes digitales contenues dans le système d'information Schengen de deuxième génération (SIS II)

1. INTRODUCTION

Il est de plus en plus difficile d'établir l'identité d'une personne en raison de changements de noms et du recours à des pseudonymes ou des documents frauduleux. Le recours à la fraude documentaire est un mode opératoire de plus en plus répandu chez les personnes qui entrent et circulent illégalement à l'intérieur de l'espace Schengen. D'après l'*analyse des risques annuelle de Frontex* pour 2015, 9 400 cas de fraude documentaire ont été recensés en 2014 à l'entrée sur le territoire de l'Union/l'espace Schengen en provenance de pays tiers, ce qui représente un léger recul par rapport à l'année précédente. Par contre, le nombre de cas rapportés lors de déplacements à l'intérieur de l'Union européenne/l'espace Schengen a nettement augmenté, passant de 7 867 cas en 2013 à 9 968 en 2014 (+27 %).

Les fraudeurs de ce type portent non seulement préjudice à la sécurité aux frontières, mais également à la sécurité intérieure de l'Union européenne. Les personnes recherchées par la police se montrent souvent évasives sur leur identité et ont recours à de nombreux pseudonymes. Certaines personnes faisant l'objet d'une interdiction d'entrée dans l'espace Schengen peuvent légalement changer d'identité dans leur pays d'origine afin d'éviter d'être repérées. Dans ce contexte, il convient de mettre en place une méthode fiable afin d'établir l'identité d'une personne. L'utilisation des empreintes digitales constituerait une méthode efficace permettant aux garde-frontières et aux agents des services répressifs d'identifier les individus recherchés par les autorités et de déceler les cas de fraude documentaire.

L'utilisation frauduleuse de documents de voyage dans le cadre des récents attentats terroristes à Paris confirme également la nécessité de mettre en place un outil permettant d'identifier les personnes sur la base de leurs empreintes digitales. Dans ce contexte, les conclusions du Conseil de novembre 2015 ont mis en évidence l'importance de renforcer les contrôles et de procéder à des vérifications systématiques. À ce jour, il n'existe pas de système à l'échelle de l'Union qui permette de vérifier l'identité d'une personne sur la base de ses empreintes digitales.

Le système d'information Schengen de deuxième génération (SIS II) est entré en service le 9 avril 2013. Il comporte une nouvelle fonctionnalité consistant en la conservation des empreintes digitales dans le système central. À l'heure actuelle, les empreintes sont utilisées pour *confirmer* l'identité d'une personne localisée à la suite de recherches, généralement sur la base de son nom ou de sa date de naissance. Il s'agit du mode de recherche «un-à-un», dans lequel les empreintes de la personne sont comparées à une série d'empreintes conservées dans le SIS. Toutefois, la possibilité d'*identifier* une personne sur la base de ses empreintes digitales requiert un ajustement des pratiques actuellement en vigueur en matière d'application des lois: il faudrait pouvoir comparer les empreintes d'une personne à toutes les séries d'empreintes (une recherche «un-à-plusieurs») afin d'identifier une personne sur la seule base de ses empreintes digitales. Cette fonctionnalité exige la mise en œuvre d'un fichier automatisé d'empreintes digitales (FAED).

Le FAED a été utilisé avec succès dans de nombreuses bases de données de coopération transfrontalière et nationale. Au sein de l'Union européenne, les exemples notables sont le système d'information sur les visas (VIS) et Eurodac.

Les articles 22, point c), de la décision SIS II[1] et du règlement SIS II[2] offrent une base juridique pour l'utilisation du FAED. Avant que cette fonctionnalité soit introduite, la Commission doit présenter un rapport précisant si la technique requise est disponible et prête à être employée; le Parlement européen est ensuite consulté. L'objectif du présent rapport est de satisfaire à cette exigence et de confirmer que la technologie d'identification des empreintes digitales est disponible et prête à être intégrée dans le SIS II.

Il convient d'évaluer le niveau de maturité et de disponibilité de la technologie d'identification des empreintes en fonction du contexte et des caractéristiques uniques du SIS II, qui présentent une série de défis techniques et organisationnels nécessitant des solutions appropriées et sur mesure. Le présent rapport, appuyé par une étude menée par le Centre commun de recherche de la Commission (JRC)[3], met également en évidence les exigences techniques et organisationnelles dans le contexte du SIS. Il décrit par ailleurs les types de scénarios dans lesquels les empreintes digitales sont utilisées de manière opérationnelle et inclut des recommandations en vue de la mise en œuvre réussie de la fonctionnalité du FAED.

2. L'ÉTUDE DU JRC ET SES RÉSULTATS

Le *programme-cadre de l'Union européenne pour la recherche et l'innovation «Horizon 2020»* décrit le niveau de maturité et de disponibilité technologiques au moyen d'une échelle allant de 1 à 9[4]: le niveau 1 représente l'observation de principes de base, tandis que le niveau 9 signifie que le système a effectivement fait ses preuves dans un environnement opérationnel. La technologie du FAED a déjà atteint le niveau 9 dans de nombreux systèmes à travers le monde.

2.1 Vue d'ensemble de la technologie du FAED

2.1.1 Performance

Le JRC a présenté une vue d'ensemble des campagnes indépendantes les plus significatives en matière d'évaluation de la performance, en recensant les initiatives pertinentes dans le contexte du SIS. Il en ressort trois concepts clés:

- le degré de précision d'un FAED est entièrement tributaire des données utilisées en vue de son évaluation, ainsi que de la qualité de ces données;

[1] DÉCISION 2007/533/JAI DU CONSEIL du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

[2] RÈGLEMENT (CE) N° 1987/2006 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

[3] http://publications.jrc.ec.europa.eu/repository/handle/JRC97779

[4] https://ec.europa.eu/research/participants/portal/doc/call/h2020/common/1617621-part_19_general_annexes_v.2.0_en.pdf
http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf

- d’autres facteurs qui peuvent influencer la performance d’un FAED sont la taille de la base de données servant aux recherches, le nombre d’empreintes utilisées aux fins de la recherche et le temps de réponse prévu;
- compte tenu de la bonne qualité des données et des recherches de type «empreinte décadactylaire par rapport à une empreinte décadactylaire», les campagnes d’évaluation ont montré que la technologie du FAED présente un degré de précision très élevé, affichant des taux d’erreur se situant autour de 0,1 %.

2.1.2 Qualité

De nombreuses études et évaluations comparatives ont révélé que la performance des systèmes biométriques dépend de la qualité des échantillons d’entrée. L’amélioration de la qualité peut être d’ordre technique, normatif, ou encore liée à la méthode d’obtention des empreintes, à savoir le scannage électronique («live-scan») ou le relevé d’empreintes manuel à l’encre. Le scannage électronique, réalisé sous la supervision d’un opérateur expérimenté, est la méthode privilégiée pour obtenir la meilleure qualité. Cependant, les relevés d’empreintes à l’encre numérisés dans la base de données existent toujours. Les systèmes devraient être dotés de processus visant à déceler les empreintes de mauvaise qualité.

Il convient de se concentrer sur la qualité de bout en bout en ce qui concerne:

- le relevé des empreintes;
- l’évaluation technique de leur qualité;
- les solutions systémiques visant à garantir une concordance;
- l’utilisation des meilleurs échantillons;
- le suivi de la performance du système et de ses utilisateurs.

La portée globale de l’étude a également permis d’aborder le point le plus délicat eu égard à la qualité: les empreintes «latentes» relevées sur les scènes de crimes ou d’accidents.

Les empreintes latentes sont exclusivement utilisées à des fins de consultation. Il est prévu de ne conserver dans le SIS que les séries complètes d’empreintes décadactylaires de personnes connues.

Dans la plupart des États membres visités, la qualité est également assurée au moyen d’«ensembles de données multiples». Lorsque les empreintes digitales d’une personne ont été relevées à plusieurs reprises, par exemple lors de chaque arrestation, celles-ci sont conservées. Chaque empreinte composant les séries peut être comparée en fonction de son score de qualité, de même qu’il est possible de compiler une série composite à partir des empreintes décadactylaires affichant la meilleure qualité. Une approche de ce type pourrait être appliquée dans le SIS.

Un point sensible concerne l’inclusion de mécanismes de mesure de la qualité dans un FAED en vue d’en améliorer la performance. Eu égard à la qualité, il convient de tenir compte des six concepts clés suivants:

- la performance d'un FAED est totalement tributaire de la qualité des données (c'est-à-dire les échantillons d'empreintes) qu'il utilise;
- de nombreux facteurs peuvent influencer la qualité des empreintes. Certains d'entre eux sont contrôlables (par exemple la propreté du capteur), d'autres non (par exemple l'usure du bout des doigts due à un travail manuel);
- les mécanismes automatiques de qualité des empreintes digitales jouent un rôle essentiel dans le contrôle de la qualité des données entrées dans un FAED;
- les différents types d'empreintes présentent des degrés de qualité différents. Les principaux types d'empreintes traités dans le cadre d'un FAED sont les suivants: les empreintes à l'encre/scannées en direct et les empreintes roulées/à plat/latentes;
- du point de vue de la performance des FAED, les empreintes latentes sont les plus complexes, car il n'existe aucun contrôle de leur qualité;
- bien qu'il n'existe pas de méthode standard pour mesurer la qualité des empreintes, les normes *NFIQ* et *NFIQ-II* relatives à la qualité de l'image des empreintes de l'Institut national des normes et des technologies des États-Unis (NIST) sont devenues des normes de facto en raison de leur très haut niveau avéré de performance et de disponibilité.

2.2 Utilisation courante de FAED nationaux

L'étude présente les cas types d'utilisation des empreintes digitales. Le cas le plus représentatif aux fins du SIS concerne une personne présente au moment de l'obtention des empreintes, par exemple un suspect ayant fait l'objet d'une arrestation. Il convient de définir deux paramètres:

- le degré de précision minimal attendu du processus de concordance;
- le temps de réponse maximal autorisé.

Par exemple, un suspect est arrêté et emmené au commissariat de police où il est soumis à un relevé d'empreintes. La série d'empreintes décadactylaires est utilisée à des fins de recherche dans la base de données centrale d'empreintes digitales. Une concordance est confirmée avec une série d'empreintes décadactylaires prise lors d'une précédente arrestation. La personne était présente à chaque relevé d'empreintes, et l'on peut donc s'attendre à un niveau élevé de qualité. Cette personne étant susceptible d'être retenue en détention pendant plusieurs heures, il n'est pas nécessaire d'avoir un temps de réponse rapide.

À titre de comparaison, lorsqu'un contrôle rapide est exigé, par exemple au guichet de contrôle d'un aéroport, deux empreintes de doigts sont peut-être seulement scannées.

Le degré de précision attendu est moindre, mais le contrôle reste significatif en ce qui concerne le relevé des deux empreintes et les séries complètes d'empreintes décadactylaires utilisées pour la comparaison. Dans ce cas, une réponse rapide est attendue – sans doute une question de secondes bien plus que de minutes – puisque la personne n'est pas en état d'arrestation. En cas de concordance, une vérification de deuxième ligne peut être effectuée au moyen d'une recherche sur la base de l'empreinte décadactylaire complète.

2.3 Eurodac et VIS

Les deux systèmes européens existants qui ont recours au FAED ont été étudiés afin de tirer d'éventuels enseignements pour le SIS.

Selon le rapport annuel 2014 de l'eu-LISA, Eurodac a enregistré 2,7 millions d'empreintes digitales (empreintes décadactylaires) et un total de 756 368 opérations ont eu lieu. En raison de procédures de qualité intégrées, le taux de refus d'empreintes ne satisfaisant pas aux normes s'élevait à 4,49 %, nécessitant de relever et soumettre à nouveau les empreintes. La taille de la base de données est proche du potentiel du SIS, mais le volume des opérations est bien inférieur et le temps de réponse nettement plus long que ne le nécessiterait le SIS – une comparaison urgente dans le système Eurodac s'effectue en l'espace d'une heure, alors que dans le SIS, le temps de réponse attendu devrait s'exprimer en secondes du fait de la grande diversité de scénarios opérationnels.

Le VIS contient près de 20 millions d'empreintes digitales (empreintes décadactylaires). En général, le VIS est utilisé pour effectuer des vérifications aux frontières, par exemple pour vérifier si la personne est bien celle qui a introduit la demande de visa. Néanmoins, le VIS est également utilisé pour effectuer des recherches «un-à-plusieurs» au sujet des nouveaux demandeurs de visa, ainsi que des vérifications de deuxième ligne aux frontières en utilisant une série complète d'empreintes décadactylaires. Chaque jour, entre 20 000 et 30 000 identifications de ce type ont lieu en moyenne, avec un taux maximal de 3 000/heure. Le temps de réponse attendu pour une identification est de moins de vingt minutes (moins de trois secondes pour une vérification «un-à-un» en utilisant entre une et quatre empreintes dans le cadre d'une vérification aux frontières classique).

2.4 FAED des États membres et des pays tiers

Selon l'étude, un FAED national appartenant à la police criminelle dans les États membres peut avoir une plus grande taille que celle prévue pour le FAED du SIS en raison de la conservation de très nombreux dossiers. Les deux systèmes étudiés aux États-Unis contiennent des dizaines de millions de dossiers. Le SIS peut quant à lui uniquement conserver des empreintes en cas de signalements de personnes. Le 1er janvier 2015, le SIS comptabilisait un peu moins de 800 000 signalements de personnes.

2.5 Les difficultés liées à la mise en œuvre de la technologie du FAED

Les difficultés liées à la mise en œuvre de la technologie du FAED peuvent être résumées comme suit:

- les cas d'utilisation;
- la performance;
- la qualité;
- la vitesse (temps de réponse);
- la taille de la base de données;
- la capacité de concordance;
- le nombre d'opérations/concordances aux périodes de pointe de la demande;

- la stratégie de gestion des requêtes;
- les formats d'échange;
- l'architecture de système: centralisée ou sur plusieurs sites;
- le type de données traitées – format de l'empreinte;
- les empreintes latentes.

2.6 Conclusions

Comme indiqué dans l'introduction du présent chapitre, la technologie est disponible et prête à être utilisée. La Commission a également mis en évidence les défis à relever. Les recommandations en vue d'assurer une mise en œuvre réussie et de relever ces défis sont décrites au chapitre 4.

3. LE FAED DANS LE SIS

Le FAED du SIS doit être en mesure de traiter tous les types de dossiers d'empreintes digitales qui seront générés. Cela inclura:

- les empreintes à plat et roulées;
- les vérifications rapides ne concernant que le scannage de deux doigts, par exemple;
- les empreintes latentes relevées sur une scène de crime.

3.1 Protection des données

Tout traitement d'empreintes digitales dans le cadre du SIS II, y compris la conservation et l'utilisation à des fins d'identification, doit être conforme aux dispositions applicables en matière de protection des données prévues par les instruments juridiques du SIS II, ainsi qu'aux dispositions nationales applicables en la matière mettant en œuvre la directive 95/46/CE[5] et la décision-cadre 2008/977/JAI[6]. Ces deux instruments juridiques s'appliquent au traitement des empreintes digitales de ressortissants de pays tiers et de citoyens de l'Union. Toute utilisation des empreintes digitales doit être autorisée par le droit de l'Union ou des États membres. Conformément au principe de spécification de la finalité, la finalité et la méthode d'utilisation des empreintes digitales dans le SIS II doivent être clairement définies. Le traitement des empreintes digitales ne doit pas excéder ce qui est nécessaire pour atteindre l'objectif d'intérêt général poursuivi, et doit faire l'objet de garanties appropriées, le cas échéant. La mise en œuvre de ces nouvelles fonctionnalités dans le SIS II devrait respecter les principes de la protection des données par défaut et dès la conception.

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

[6] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

3.2 Scénarios d'utilisation des empreintes digitales dans le SIS

Le SIS prévoit deux types d'opérations concernant les empreintes digitales:

- la création/mise à jour d'un signalement, accompagnée des empreintes;
- la consultation de la base de données SIS sur la base des empreintes plutôt que du nom et de la date de naissance. Cette consultation est également effectuée avant l'introduction d'un nouveau signalement, afin de vérifier si la personne est déjà listée dans le SIS sous un autre signalement.

Lorsqu'elles sont disponibles, les empreintes doivent être jointes aux signalements du SIS. Les circonstances dans lesquelles des empreintes peuvent figurer dans le SIS sont présentées dans les sous-chapitres suivants. Tous les cas ont été comparés à des «cas d'utilisation» similaires qui avaient déjà été traités dans les FAED des États membres. En fonction du scénario, les différents cas sont déjà largement couverts par le cas d'utilisation présenté dans l'étude du JRC décrivant les vérifications de type «empreinte décadactylaire par rapport à une empreinte décadactylaire».

À moins qu'un cas ne mette en évidence une difficulté opérationnelle, la qualité des empreintes est généralement élevée, puisque les empreintes récemment obtenues d'une personne et la série d'empreintes conservée dans la base de données ont été relevées dans des conditions contrôlées, avec la possibilité de rejeter les empreintes de mauvaise qualité pour les relever à nouveau.

Lorsqu'un État membre introduit un signalement, mais ne dispose pas d'empreintes pour le compléter, il est possible qu'un autre État membre ayant déjà eu affaire à la personne conserve ses empreintes dans son FAED national. Le manuel Sirene[7] fournit des instructions pour la transmission des empreintes qui doivent accompagner le signalement. Étant donné que les empreintes sont susceptibles d'avoir été relevées dans un autre système, il convient de veiller à ce qu'elles contiennent une trace de leur «score de qualité», de sorte que toute utilisation des empreintes ait lieu dans un contexte éclairé.

3.2.1 Non-admission ou interdiction de séjour (article 24 du règlement)

Ce type de signalement est de loin le plus courant. Dans l'hypothèse où la personne visée par un signalement dans le SIS (personne signalée) est à la disposition de l'État membre signalant, son empreinte décadactylaire sera relevée, jointe au signalement et comparée avec les fiches décadactylaires déjà contenues dans le SIS. Cela permettrait d'établir des liens avec d'autres signalements.

3.2.2 Arrestation aux fins de remise ou d'extradition (article 26 de la décision)

Si la personne signalée n'est pas accessible au moment du signalement, ses empreintes ne seront pas disponibles. Néanmoins, il se peut que l'État membre signalant les possède déjà dans son FAED national et qu'il soit en mesure de compléter le signalement. L'empreinte décadactylaire

[7] Annexe de la décision d'exécution 2013/115/UE relative au manuel Sirene et à d'autres mesures d'application pour le système d'information Schengen de deuxième génération (SIS II).

sera relevée, jointe au signalement et comparée avec les fiches décadactylaires déjà contenues dans le SIS.

3.2.3 Personnes disparues (article 32 de la décision)

Les empreintes de personnes disparues ne sont pas toujours disponibles au moment de la création d'un signalement. Toutefois, dans certains cas, s'il existe un registre national et que la législation le permet, les empreintes peuvent être transférées à un signalement.

En cours d'enquête, les empreintes latentes d'une personne peuvent être utilisées pour interroger le SIS (mais ces empreintes ne seraient pas conservées ni stockées dans la base de données). Dans ce cas, il ne s'agit pas de la création d'un signalement, mais d'une consultation.

3.2.4 Personnes recherchées dans le but de rendre possible leur concours dans le cadre d'une procédure judiciaire (article 34 de la décision)

Les empreintes pourraient ne pas toujours être disponibles; un État membre peut cependant compléter le signalement grâce aux empreintes contenues dans son FAED national, lorsque la situation le permet.

3.2.5 Contrôle discret ou contrôle spécifique (article 36 de la décision)

Dans certains cas, il se peut que les empreintes ne soient pas disponibles. Selon la nature des contrôles, les empreintes sont susceptibles de ne pas être accessibles à un stade ultérieur. Néanmoins, il se peut que l'État membre signalant possède déjà ces empreintes dans son FAED national et qu'il soit en mesure de compléter le signalement. Les contrôles de police/aux frontières offrent la possibilité d'effectuer une recherche sur la base de ces empreintes.

3.2.6 Usurpation d'identité (article 36 du règlement; article 51 de la décision)

Avec le consentement de la personne dont l'identité a été usurpée, les États membres peuvent ajouter ses empreintes dans le signalement de la personne qui a usurpé son identité. Cette procédure suppose la «mise à jour» d'un signalement, et non sa «création». Elle permet aux autorités d'identifier à la fois l'usurpateur et la victime, puisque cette dernière est en mesure de prouver son identité, le cas échéant. À la suite d'un résultat positif à une recherche sur la base du nom et de la date de naissance lors d'un contrôle de première ligne aux frontières, l'identité de la victime peut être vérifiée au moment de la vérification de deuxième ligne.

3.3 Quantifier la taille du FAED du SIS et le nombre d'opérations

Au moment de la réalisation de l'étude, le SIS contenait environ 5 500 dossiers d'empreintes digitales. Les États membres ont confirmé que l'absence de la fonctionnalité d'un FAED constituait un facteur limitatif au téléchargement d'empreintes dans le SIS.

3.3.1 Taille

Le nombre de signalements de personnes dans le SIS est relativement stable. Ce nombre est susceptible d'augmenter en raison des propositions visant à ajouter des signalements concernant des décisions de retour et les interdictions d'entrée y afférentes. Même dans ce cas, on estime que la taille du FAED du SIS sera inférieure à celui d'un grand État membre et qu'elle ne posera, par conséquent, aucun problème technique.

3.3.2 Volume des opérations

Il convient de tenir compte des trois types d'opérations suivants:

- **Requêtes/consultations.** Le plus grand nombre de demandes dans le SIS concernera des requêtes/consultations. En 2014, près de deux milliards de requêtes, concernant toutes les catégories de signalement, ont été envoyées au SIS, soit dans des copies nationales soit au système central. Cela inclura les consultations, déjà envoyées au SIS, qui seront appuyées par l'introduction d'un FAED. Les demandes de visa introduites par l'intermédiaire du VIS devraient faire l'objet d'une vérification par rapport au SIS. Entre 20 000 et 30 000 requêtes d'identification sont effectuées chaque jour. En 2014, Eurodac a traité 750 000 opérations. Avant de procéder à ces opérations, il convient de consulter le VIS et le SIS à des fins de prévention, de détection et d'enquête sur des actes de terrorisme et d'autres infractions pénales graves. Il est également prévu d'effectuer des vérifications d'empreintes digitales. Les contrôles aux frontières de Schengen sont réalisés sur la base du nom et de la date de naissance. À l'avenir, pour les ressortissants de pays tiers, il est envisagé d'effectuer des vérifications d'empreintes digitales. Toutes les requêtes sur des personnes ne peuvent pas être introduites selon cette méthode, puisque les signalements ne contiennent pas tous des empreintes; un grand nombre de contrôles continueront donc à être menés sur la base du nom et de la date de naissance. Tous les points d'accès au SIS ne peuvent pas effectuer des requêtes sur la base d'empreintes.

- **Création/mise à jour/suppression (CMS) de signalements.** En 2014, 1,4 million d'opérations CMS ont été enregistrées. Parmi celles-ci, 780 000 concernaient la création et la mise à jour de signalements de personnes et ont pu, par conséquent, donner lieu à l'ajout d'empreintes. La suppression devrait consister en un processus automatisé lors de la suppression d'un signalement, mais les demandes de traitement devraient être tout simplement intégrées.

Il importe de veiller à la disponibilité de statistiques précises afin de définir adéquatement la taille du FAED du SIS. Le savoir-faire acquis lors de la mise au point des FAED nationaux peut être utilisé dans le cadre du SIS.

3.3.3 Normes relatives à l'échange d'empreintes digitales

Les normes du NIST et le guide des meilleures pratiques d'Interpol fournissent une base adéquate pour ce type d'échange.

3.3.4 Architecture

L'architecture du SIS comprend les éléments suivants:

- un système central traitant 20 % des opérations – cinq États membres utilisent directement le système central;
- des copies nationales (80 % des opérations) qui peuvent être:
    - «partielles» (qui ne contiennent que des données composées de mots et de chiffres – neuf États membres disposent de ce type de copies), ou
    - «complètes» (qui contiennent des données composées de mots et de chiffres, ainsi que de photographies et d'empreintes – seize États membres disposent de ce type de copies).

Un FAED central est nécessaire pour fournir des services aux États membres qui ne possèdent pas de copie nationale, aux États membres qui possèdent une copie nationale partielle ou encore aux États membres qui sont confrontés à une indisponibilité technique de leur copie nationale complète.

Toutes les opérations CMS portant sur des signalements relèvent du système central. L'ajout d'empreintes à un signalement requerra un contrôle de la qualité du FAED au niveau du système central.

Les opérations CMS réalisées dans le système central sont répercutées en trois minutes dans les copies nationales. Il conviendra de mettre en place un FAED central pour appuyer ces opérations.

Conformément aux instruments juridiques du SIS II, une recherche dans une copie nationale doit produire un résultat équivalent à celui d'une recherche dans la base de données du SIS. Le respect de ce principe applicable aux recherches fondées sur des noms et des chiffres doit être observé dans le cadre de recherches sur la base d'empreintes digitales.

Si un État membre met en œuvre son propre FAED dans le cadre d'une copie nationale, ce dernier doit offrir les mêmes performances en termes d'identification que celles du FAED central. Sur les plans technique et juridique, il est possible de disposer d'un FAED dans le cadre d'une copie nationale, mais il sera difficile de garantir l'équivalence des résultats.

Il est plus facile de gérer une architecture centralisée du point de vue de la qualité, mais elle doit être en mesure de traiter les demandes qui lui sont soumises. Une architecture composée d'un FAED central et d'autres FAED contenus dans des copies nationales complètes permettrait de répartir les demandes, mais elle serait confrontée aux mêmes difficultés que celles exposées ci-dessus. Ces difficultés pourraient être résolues grâce à des FAED de ce type utilisant tous le même logiciel.

Après avoir décidé d'une architecture générale, il conviendra de déterminer si les cas d'utilisation devront être traités de la même façon ou si des différences en termes de volume ou de temps de réponse favoriseraient des axes de travail ou des sous-systèmes parallèles au sein du FAED.

Certaines opérations de contrôle aux frontières et d'application de la loi exigeront un temps de réponse inférieur à 30 secondes, mais celui-ci devrait seulement être inférieur à cinq minutes à un poste consulaire.

Dans le contexte de contrôles effectués dans des commissariats de police, un temps de réponse inférieur à dix minutes pourrait être exigé. Il est important d'évaluer la charge de travail prévue dans ces cas d'utilisation et de définir des priorités dans le traitement des demandes. L'utilisation de filtres, comme l'âge et le sexe, permet de réduire le nombre de dossiers à comparer, améliorant ainsi le temps de réponse.

Enfin, le FAED du SIS devra s'inscrire dans le cadre des procédures d'évaluation et de rapport établies dans les instruments juridiques du SIS II.

4. RECOMMANDATIONS

Les précédents chapitres confirment la maturité et la disponibilité de la technologie du FAED. En outre, la Commission estime qu'il convient d'envisager la mise en œuvre des 19 recommandations suivantes afin de favoriser le bon déploiement et la bonne utilisation d'un FAED dans le SIS.

1. **Nécessité de disposer de statistiques complémentaires** – eu égard au nombre de consultations/année portant sur des personnes et à leur contexte opérationnel, afin d'évaluer correctement la taille et la puissance de traitement du FAED.
2. **Promotion de meilleures pratiques** – pour le FAED du SIS, fondée sur le savoir-faire acquis lors de la mise au point et de la gestion des FAED nationaux.
3. **Norme commune en matière d'échange** – les normes du NIST offrent une base appropriée pour l'échange de données dactyloscopiques. Il convient de mettre en place un contrôle automatique en ce qui concerne sa mise en œuvre.
4. **Complémentarité entre la décision Prüm et le SIS II –** il convient de préciser la nature complémentaire du mécanisme de Prüm et du FAED du SIS afin d'éviter tout double emploi[8].
5. **Sous-systèmes dédiés** – au vu de la diversité des cas d'utilisation, notamment en ce qui concerne le volume et le temps de réponse, il convient d'envisager des axes de travail parallèles ou des sous-systèmes dédiés.
6. **Processus d'enregistrement de haute qualité** – la phase d'enregistrement devrait privilégier l'utilisation de dispositifs de scannage en direct («live-scan») par des opérateurs chevronnés.
7. **Stockage de séries de données multiples** – afin de favoriser une stratégie de concordance composite.

[8] Les empreintes digitales conservées dans le SIS II sont jointes aux signalements et l'accès au SIS II est requis lors de contrôles et de vérifications aux frontières effectués par les autorités répressives. Sur la base de la décision 2008/615/JAI, le mécanisme de Prüm prévoit la possibilité d'interroger les FAED nationaux en matière pénale. Contrairement au SIS II, le mécanisme de Prüm ne prévoit pas la possibilité d'accéder en temps réel aux dossiers d'empreintes et ne peut être utilisé que dans des enquêtes individuelles.

8. **Transfert contrôlé de séries de données** – le FAED du SIS devrait accepter les empreintes générées dans d'autres systèmes, pour autant que les paramètres desdits systèmes soient conservés dans la série de données incluse dans le signalement.
9. **Qualité des points de capture**
    a. **Supervision par un opérateur -** formation appropriée pour l'enregistrement
    b. **Capteur adéquat** - il convient de privilégier les dispositifs de scannage en direct («live-scan»).
    c. **Interface utilisateur graphique (IUG) améliorée –** afin d'offrir un retour d'informations en temps réel sur les données acquises.
    d. **Interaction appropriée avec l'utilisateur** - le processus d'enregistrement devrait être convivial.
    e. **Environnement adéquat** - en termes d'éclairage, de température et de contexte
    f. **Entretien du capteur –** il doit être réalisé sur une base régulière et systématique.
10. **Algorithmes pour l'évaluation de la qualité**
    a. **Respect des normes –** l'utilisation de métriques de qualité reconnues.
    b. **Actions correctrices –** aux fins de l'obtention d'empreintes de qualité satisfaisante
11. **Qualité des systèmes d'identification**
    a. **Traitement fondé sur la qualité** - comprenant l'utilisation d'outils supplémentaires, comme des fonctions d'extraction alternatives et des algorithmes de concordance liés à des processus spécifiques.
    b. **Fusion fondée sur la qualité** - la combinaison de différents échantillons afin d'être en mesure de procéder à des vérifications composites.
    c. **Remplacement/mise à jour des modèles –** l'utilisation des meilleurs échantillons lors de la production de modèles pour l'établissement d'un FAED.
    d. **Suivi –** la constitution de statistiques pour chaque type d'application; sites, dispositifs et opérateurs.
12. **Cas concernant des enfants –** notamment dans le cas de personnes disparues, le FAED du SIS devrait être capable de moduler le processus de concordance lorsqu'il apparaît clairement que l'enfant a grandi depuis le relevé d'empreintes.
13. **Service centralisé de contrôle de la qualité** - afin de confronter la qualité des empreintes aux métriques de qualité du FAED du SIS.
14. **Communication d'information sur des fiches décadactylaires de qualité inférieure** - lorsqu'une série de données, proposée à des fins d'enregistrement ou d'ajout dans un signalement, n'obtient pas le niveau de qualité requis pour le FAED du SIS, que ce soit dans un signalement ou dans la fiche de données elle-même.
15. **Intégrité de la base de données** - recours aux meilleures pratiques afin de réduire le risque d'incohérences ou de données erronées, y compris les empreintes, enregistrées dans la base de données.
16. **Consultation**

a. **Résolution optimisée (1000 ppp[9]) -** afin de pouvoir conserver les empreintes de meilleure résolution qui seront produites par les États membres lorsque ces derniers auront mis à niveau leurs scanneurs.

b. **Empreintes digitales à plat et roulées -** il convient d'autoriser les États membres, à des fins de consultation seulement, à limiter le relevé d'empreintes aux empreintes à plat.

c. **Contrôle rapide sur la base de deux empreintes -** la possibilité d'effectuer des consultations rapides.

17. **Temps de réponse appropriés** – afin de respecter les trois temps de réponse indicatifs fondés sur les différents scénarios opérationnels, à savoir: a) très court (c'est-à-dire inférieur à 30 secondes); b) moyen (c'est-à-dire inférieur à cinq minutes); c) plus long (c'est-à-dire jusqu'à 10 minutes).

18. **Priorité des requêtes** - la définition de niveaux de priorité pour le traitement des requêtes en vue d'une meilleure gestion de la charge de travail du système par le FAED du SIS.

19. **Comparaison des performances** – prise en considération, à un stade précoce, de la programmation d'évaluations de la performance du FAED du SIS.

5. PROCHAINES ÉTAPES – PLAN D'ACTION

L'achèvement de l'étude et la présentation du présent rapport au Parlement européen à des fins de consultation constituent les premières étapes vers l'introduction d'une fonctionnalité de FAED dans l'environnement du SIS. Dans la pratique, la description détaillée des activités désormais attendues de la part de l'eu-LISA et des États membres peut se résumer comme suit:

(1) définir les exigences relatives au contrôle de qualité spécifique afin de vérifier que les données répondent à une norme de qualité minimale. Les spécifications devraient être incluses dans une décision d'exécution de la Commission;

(2) finaliser les exigences relatives aux utilisateurs et la détermination de la taille du système requis;

(3) définir l'architecture du système requis. Celle-ci devrait être incluse dans une décision d'exécution de la Commission;

(4) définir les spécifications techniques et le calendrier de mise en œuvre;

(5) exécuter le projet menant à la mise en œuvre du FAED du SIS.

6. CONCLUSION

Un lien intrinsèque a déjà été établi entre la fonctionnalité d'un FAED et les bases de données des services répressifs et aux frontières. Le SIS représente l'une de ces bases de données et les signalements de personnes ne seront pas pleinement performants et utiles sans l'appui d'un FAED.

[9] Points par pouce.

À la lumière de l’analyse et des observations synthétisées dans le présent rapport, la Commission conclut que la technologie du FAED a atteint un degré de maturité et de disponibilité suffisant pour être intégrée dans le SIS. Le présent rapport fournit également une vue d’ensemble des suggestions de la Commission dont il faudra tenir compte lors de la mise en œuvre et de l’utilisation du FAED du SIS dans un environnement opérationnel.