FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Monographie | EUROPE

Ligue des droits de l'Homme
FONDÉE EN 1898

aedh

Humanistische Union

HUNGARIAN CIVIL LIBERTIES UNION
HCLU

Ligue des Droits de l'Homme
Action Luxembourg Ouvert et Solidaire

MEDEL
Magistrats Européens pour la Démocratie et les Libertés

Avril 2014

1. INTRODUCTION GÉNÉRALE

Le fichage institutionnel est aussi pratiqué au niveau de l'Union européenne (UE). Cette monographie présente quatre systèmes européens impliquant le fichage d'individus : le Système d'Information Schengen II (SIS II) relatif aux personnes recherchées ou exclues du territoire de l'Union européenne, le Système d'Information Visa (VIS) relatif aux demandeurs de visa, le système EURODAC relatif aux demandeurs d'asile et le système ECRIS relatif aux casiers judiciaires.

Ces systèmes couvrent une très grande partie de la population présente sur le territoire de l'Union européenne, qu'il s'agisse de personnes ressortissantes de l'UE ou non.

Malgré le fait qu'ils émanent tous de « politiques communes », ECRIS se distingue des trois autres systèmes par son fonctionnement (décentralisé dans chaque État membre), sa gestion (principalement nationale) et son régime en ce qui concerne la protection des données (émanant de la Décision cadre du Conseil 2008/977/JAI du 27-11-2008).

Présentation des cadres européens sur la protection des données.

1.1. La Directive 95/46/CE[1]

La **Directive 95/46/CE** du Parlement européen et du Conseil sur le traitement des données personnelles et la libre circulation de ces données **communément appelée Directive 95** établit les règles et les principes régissant tout traitement des données personnelles effectué par le secteur privé ou public, à l'exception des traitements qui ne relèvent pas du droit communautaire (police, justice criminelle, etc.), ainsi que les droits des individus et les obligations des responsables du traitement.

La Directive établit les principes généraux applicables à tout traitement licite des données personnelles, à savoir le principe du consentement de la personne concernée, le principe de légalité, le principe de finalité, le principe de proportionnalité, le principe de la précision (accuracy principle), le principe de minimisation des données et le principe de la limitation de la durée du traitement. Elle précise que toute personne a :

• le droit d'être informée des conditions de la collecte et de la mise en traitement de ses données personnelles, le droit d'accès aux données personnelles collectées sur sa personne, le droit de rectification des données qui seraient erronées ;

• le droit de s'opposer au traitement de ses données pour motif impérieux ;

• et le droit de ne pas être soumis à une décision l'affectant de manière significative, prise sur seule base d'un traitement automatisé de ses données destiné à évaluer certains aspects de sa personnalité.

En outre, la Directive prévoit les obligations respectives de tout responsable de traitement, à savoir :

• l'obligation de traiter les données en conformité avec les principes généraux du traitement, l'obligation d'informer la personne concernée,

• l'obligation de respecter la confidentialité et la sécurité des données

• et l'obligation de notifier à l'autorité de contrôle tout traitement des données personnelles selon la législation nationale applicable.

La Directive prévoit des règles pour le transfert international des données personnelles, basé sur le concept de la protection adéquate assurée par le pays tiers.

La Directive prévoit également des règles sur le droit de chaque personne concernée de porter plainte pour la violation de ses droits et des règles sur la possibilité de faire des recours administratifs et juridictionnels. Elle prévoit aussi des sanctions en cas de violation de ces règles et principes. En outre,

1. La présente contribution se base sur les textes disponibles au moment de la rédaction (novembre 2013), la Directive n°95/46/CE et les propositions de réforme initiales de la Commission européenne du 25 janvier 2012. Les textes initiaux ont été amendés et votés au Comité LIBE du Parlement européen le 21 octobre 2013. La version adoptée n'avait pas encore été rendue disponible.

elle inclut aussi des règles relatives au contrôle indépendant en ce qui concerne tout traitement des données personnelles au niveau national mais aussi la coopération des autorités de contrôle au niveau européen.

Ainsi, les données des personnes qui sont traitées par des entreprises ou les administrations établies dans l'Union européenne ne peuvent être traitées que dans les circonstances prévues par la Directive et c'est sous ces conditions qu'est garantie la libre circulation des données dans l'Union.

La Directive est actuellement en cours de réforme. Cette réforme a été jugée nécessaire par la Commission européenne en raison des évolutions technologiques qui ont modifié en profondeur la façon dont les données personnelles sont collectées, traitées et échangées dans le nouvel environnement numérique ainsi qu'en raison de la globalisation où les données à caractère personnel sont devenues un atout essentiel pour les activités économiques des entreprises. Le but étant de construire un espace commun où les droits des individus seraient renforcés dans un contexte de sureté juridique et de libre circulation pour les entreprises.

Cette réforme prévoit de nouveaux concepts comme le droit a l'oubli numérique, le droit de la portabilite numérique, l'obligation pour le responsable du traitement d'appliquer les mécanismes de « respect de la vie privée dès la conception » (« privacy by design ») et du « respect de la vie privée par défaut » (« privacy by default »), l'interdiction du profilage, l'obligation de mettre en oeuvre des évaluations d'impact sur la protection des données (« data protection impact assesssments »), l'obligation pour les grandes entreprises et l'administration publique de désigner un responsable de la protection de la vie privée (« privacy officer »), l'obligation du responsable du traitement de tenir un registre de tous ses traitements et l'obligation de notifier toute violation de securité à la personne concernée et à l'autorité de contrôle.

Le règlement sera complété par une Directive sur la protection des données dans le cadre de la coopération judiciaire et policière en matière pénale. Ce domaine est actuellement régi par la Décision cadre du Conseil 2008/977/JAI du 27-11-2008.

La réforme de la Directive a amené de nombreux débats. Lors de la rédaction de ce document[2] le projet de réforme n'a pas encore abouti et la fin proche du mandat des parlementaires européens ne permet pas de présager de sa forme finale. Le Comité LIBE (Libertés Civiles, Justice et Affaires Intérieures) du Parlement européen a transmis ses propositions de textes au Conseil, où les discussions sont en cours.

1.2. Les autorités de protection des données de l'Union européenne

Un élément important du régime de protection est l'établissement d'un système indépendant de contrôle. Ceci comprend :

Le **Contrôleur Européen de la Protection des Données** (CEPD) : il contrôle les traitements de données à caractère personnel effectués par les institutions et les organes de l'UE ; donne des conseils sur les politiques et les textes législatifs qui touchent à la vie privée ; coopère avec les autorités de protection des données afin de garantir une protection des données cohérente[3].

Si le rôle de supervision des institutions et organes européens donne un pouvoir d'influence important et coercitif au CEPD, son rôle de conseil n'a qu'une portée consultative et ce même si ses études d'impact, ses avis préalables, ses avis formels et ses observations sont sans complaisance. Il a aussi le pouvoir, peu utilisé, de saisine de la Cour de Justice de l'Union Européenne. Son rôle de coopération, en particulier au sein du Groupe de Travail Article 29 (Groupe 29), lui assigne un rôle de promotion d'application cohérente des règles de protection des données personnelles dans tous les pays de l'UE. Son rôle en matière de coopération policière et judiciaire est limité à promouvoir le respect de la protection des données dans ce domaine. Il a néanmoins un rôle de contrôle partagé avec les autorités nationales en ce qui concerne Eurodac. Beaucoup espéraient que la proposition de réforme, par la Commission européenne, de la directive 1995 élargirait les compétences propres du CEPD, notamment en matière

2. Novembre 2013
3. Compétences reprises sur le site internet du CEPD

de coopération policière et judiciaire. Il n'en est a priori rien. Une timide ouverture semble se dessiner à la suite des amendements proposés au Conseil par le Comité LIBE du Parlement européen, mais cela reste bien en deçà des propositions qui ont pu être faites par les défenseurs des droits et libertés.

Le **Groupe de Travail Article 29 (Groupe 29),** créé en vertu de l'article 29 de la Directive 95/46/CE, est un organe consultatif et indépendant auprès de la Commission Européenne, composé, d'un représentant de chaque autorité nationale de protection des données, du CEPD et d'un représentant sans droit de vote de la Commission[4]. Il donne des avis d'expert, promeut l'uniformisation de la protection des données dans les États membres au moyen de recommandations sur tout sujet qu'il considère comme important (notamment en matière de technologies nouvelles). Ses avis et rapports font autorité. Le groupe est notamment chargé d'examiner toute question relative aux mesures nationales adoptées en accord avec la Directive 95/46/CE en vue de leur application homogène au niveau européen, et d'informer la Commission en cas de divergences entre les pratiques des États membres. Il est également chargé de donner son avis, rendu public, sur le niveau de protection des données assuré dans les pays tiers.

La proposition de Règlement général sur la protection des données établit un **Comité européen indépendant de la protection des données** comme le successeur du Groupe 29[5]. La proposition prévoit des compétences renforcées pour ce Comité, en comparaison de celles du Groupe 29, afin de favoriser l'application cohérente du Règlement, notamment via l'établissement de lignes directrices, destinées aux autorités nationales de protection des données et via l'émission d'un avis à destination de toute autorité nationale de protection des données traitant d'une mesure ayant un impact européen dans le cadre du nouveau mécanisme de contrôle de la cohérence[6].

La proposition de Directive sur la protection des données dans le cadre de la coopération judiciaire et policière prévoit des compétences relativement similaires à celle prévues dans la proposition de Règlement, notamment une mission générale de coordination des autorités nationales de protection des données[7].

Les autorités nationales de protection des données, mises en place par chaque État membre sont chargées de superviser territorialement la mise en œuvre et l'application au niveau national de la Directive 95. Elles ont un pouvoir d'investigation, d'intervention et sont habilitées à engager des poursuites légales. Elles souffrent souvent de manque de moyens. Les marges de manœuvres laissées aux États membres par la Directive 95 ont entrainé des différences notables dans les pouvoirs conférés à ces autorités ainsi que dans les procédures que doivent respecter les responsables de traitement, le Groupe 29 étant seulement un cadre de discussion sans effet contraignant.

Le projet de réforme en cours introduit le **principe de « guichet unique »** selon lequel seule l'autorité de contrôle du pays dans lequel une entreprise qui a des établissements dans plusieurs États membres a son établissement principal sera compétente pour décider au cas de violation du droit. Cette décision serait quand même consultée avec les autres autorités de contrôle nationales selon un mécanisme de coopération. Les avis du Comité européen de la protection des données sont prévus et une intervention contraignante de la Commission européenne[8] est également prévue en cas de désaccord. Au moment de la rédaction de cette monographie les discussions au Conseil sont en pleine évolution et on ne connait pas la procédure exacte de ce mécanisme.

Dans le cadre de la directive sur la protection des données en matière de coopération policière et judiciaire, les pouvoirs des autorités de contrôle seront moindres, souvent vagues et ambigus, laissant

4. Les États membres de l'Espace économique européen (Islande, Liechtenstein et Norvège) y ont le statut d'observateur, tout comme quelques candidats-membres (Croatie DEVENUE MEMBRE, ex-République yougoslave de Macédoine)
5. Proposition de Règlement général sur la protection des données, Art. 64.
6. Explicité brièvement *ci-après.* Voir aussi : Proposition de Règlement, Art. 57-60.
7. Proposition de Directive sur la protection des données en matière de coopération judiciaire, Art. 49.
8. Proposition de Règlement, Art 57

place à des interprétations nationales divergentes. Une autorité nationale de protection spécifique est prévue pour l'application de cette Directive mais les États membres auront la possibilité de désigner une autorité différente de celle prévue dans le contexte du règlement. Pourtant, l'égalité de traitement des données personnelles des citoyens de l'Union et l'efficacité du traitement devraient passer par une autorité indépendante européenne avec un réel pouvoir de contrôle, de concordance, voire de dernier recours que le CEPD pourrait bien assurer.

1.3. La Convention 108 du Conseil de l'Europe

Communément appelée la **Convention 108**, la Convention du Conseil de l'Europe (CdE) sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 est le premier instrument international juridiquement contraignant à vocation universelle dans le domaine de la protection des données. Le CdE regroupe 47 États dont les 28 États membres de l'Union européenne mais la Convention est ouverte pour ratification à tout autre État tiers[9]. Cette Convention fut développée afin d'éviter les abus de collecte et de traitement de données à caractère personnel, à la suite des progrès réalisés dans les domaines technologiques dans les années 70 qui ont permis aux administrations publiques et aux grandes entreprises de se constituer d'importantes banques de données. Son champ d'application couvre tant le secteur public que le secteur privé. La Cour Européenne des Droits de l'Homme de Strasbourg peut être saisie sur la base du non-respect des principes posés par cette convention en raison de son lien avec l'article 8 sur le droit à la vie privée de la Convention des Droits de l'Homme.

Comme, au niveau de l'Union européenne, la **Directive 95/46/CE** n'est pas applicable aux traitements des données personnelles dans le cadre de **la coopération judiciaire et policière en matière pénale**, c'est la **Décision-cadre du Conseil** 2008/977/JAI[10] qui s'applique dans le cadre d'opérations transfrontalières. Donc, dans ce secteur, la collecte des données et les opérations de traitement qui se situent au niveau national, sans aspect transfrontalier, ne sont couvertes actuellement au sein de l'Union européenne que par la Convention 108.

La Convention 108 est actuellement en cours de **modernisation** afin de faire face aux nouveaux défis technologiques, mais également afin de renforcer les mécanismes de suivi de l'application de la Convention par les États qui l'ont ratifiée, et l'ouverture à la ratification par des entités régionales, telles que l'Union européenne, ou internationales. Les propositions finales sur la modernisation de la Convention de novembre 2012 sont actuellement finalisées par un comité ad hoc pour soumission au Comité des Ministres du Conseil de l'Europe.

Le processus de modernisation commencé plus d'un an avant la proposition de réforme de la Directive 95 vise notamment à bénéficier des réflexions sur les acquis efficaces sur le plan national et régional afin de renforcer les droits des individus et de promouvoir un modèle de protection de haut niveau aux États parties du CdE. Il est aussi proposé d'inclure dans la Convention les dispositions du protocole additionnel à la Convention adopté en 2001 notamment concernant les autorités de contrôle et des principes relatifs aux transferts de données vers des pays non parties à la Convention. La nouvelle Convention intègrerait entre autres la notion de « protection de la vie privée dès la conception » de produits ou services destinés aux traitements de données et elle prévoit un mécanisme de contrôle et de suivi de sa mise en œuvre par les Parties[11].

9. Le premier État non-européen qui a ratifié la Convention récemment, est l'Uruguay, ce qui souligne sa vocation universelle.
10. En général, les dispositions de la Décision-cadre ont été critiquées car ne protégeant pas suffisamment les données des individus.
11. Le texte proposé par le comité de la convention le 18 décembre 2012 est accessible en français http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2013)01_F_vers_13_11_2013.pdf, et en anglais : http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2013)01_En_%20Working%20doc_Conv%20108%20.pdf

Le processus d'examen de cette proposition à vocation mondiale implique, à titre consultatif, de nombreux États non européens ayant déjà adopté une loi sur le droit à la protection des données personnelles, des organisations internationales, ainsi que des associations représentant des parties prenantes[12].

1.

12. http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2013)ToR_E_04%2011%202013.pdf

2. SYSTÈME D'INFORMATION SCHENGEN II (SIS II)

2.1. Cadre

2.1.1. Liens avec d'autres politiques de l'UE

2.1.1.1. La politique Schengen

La première version du Système d'Information Schengen (SIS) – résultant de la politique Schengen lancée en 1985 - a commencé à fonctionner en 1995. Cette politique consiste à supprimer les frontières intérieures afin de permettre la libre circulation des personnes au sein de l'espace Schengen, entrainant un nécessaire renforcement des frontières extérieures.

Un fichier central commun répertoriant les personnes ou objets recherchés par chacun des États membres fut donc créé, de sorte que chaque police compétente sur un territoire ou à la frontière extérieure puisse, soit leur interdire l'entrée dans l'espace dit "Schengen", soit les arrêter. Ce fichier permet également de suivre les mouvements au sein de l'espace Schengen.

La coopération entre chaque État a conduit à la signature, à Schengen (Luxembourg), de l'Accord sur l'abolition progressive des frontières internes, suivi par la signature en 1990 de la Convention mettant en œuvre l'Accord de Schengen. Au début de sa mise en œuvre, en 1995, sept pays étaient partie prenante de cet accord. Basés sur un accord intergouvernemental, les Accords de Schengen font aujourd'hui partie de la législation de l'UE.

Les États participants au SIS II sont les États membres de l'UE appartenant à la zone Schengen, au nombre de 22[13], quatre pays non-membres de l'UE mais appartenant à la zone Schengen (Islande, Lichtenstein, Norvège et Suisse) ainsi que le Royaume-Uni et l'Irlande sur les questions de coopération judiciaire et policière. Au total, 28 pays sont donc aujourd'hui acteurs du SIS II. Début 2014, la Roumanie, la Bulgarie et Chypre devaient également rejoindre la zone Schengen et par la même occasion les activités du SIS II. Pour ce qui est de la Croatie, cela dépendra de la date à laquelle le pays sera autorisé à entrer dans l'Espace Schengen.

2.1.1.2. Un outil renforcé par la lutte contre le terrorisme

Depuis les attaques terroristes du 11 septembre 2001, les États membres ont intensifié leur coopération en matière de lutte contre le terrorisme. Reconnu comme un outil important de sécurisation de l'espace Schengen, SIS a été technologiquement amélioré afin de permettre son utilisation tant dans les enquêtes liées au terrorisme que dans la prévention des attaques terroristes[14].

En plus de la participation de nouveaux États (pays de l'élargissement de l'UE et de l'EEE[15]), SIS a

13. Au 31 octobre 2013, moment de l'écriture, il s'agit de l'Allemagne, l'Autriche, la Belgique, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Slovaquie, la Slovénie et la Suède.

14. Le lien entre la mise à jour du SIS et la stratégie de l'UE en matière de lutte contre le terrorisme peut être trouvé dans le règlement (CE) No 871/2004 du 29 avril 2004 concernant l'attribution de certaines fonctions nouvelles au Système d'information Schengen, y compris dans le cadre de la lutte contre le terrorisme ; dans la décision 2005/211/JAI du Conseil du 24 Février 2005 concernant l'attribution de certaines fonctions nouvelles au Système d'information Schengen, y compris dans le cadre de la lutte contre le terrorisme, et dans la stratégie de l'Union Européenne visant à lutter contre le terrorisme.

15. Espace Economique Européen

également acquis de nouvelles fonctionnalités. Ainsi, diverses autorités, telles qu'EUROPOL[16] et EUROJUST[17] ont maintenant accès à cette nouvelle version du système, appelée SIS II. Parallèlement, de nouvelles catégories et de nouveaux types de données ont été créés, comme - par exemple - les données biométriques (photos, empreintes digitales). L'idée sous-jacente à cette refonte du SIS est de collecter plus de données et d'établir une meilleure collaboration entre les diverses autorités policières, afin de mettre en place des stratégies d'application de la loi plus efficaces.

2.1.1.3. Un outil essentiel à l'accomplissement d'un « espace de liberté, de sécurité et de justice »

L'objectif d'un espace libre, sûr et juste où les citoyens peuvent se déplacer sans obstacles (ex : sans frontière, charge administrative ou discrimination) est inscrit dans les stratégies pluriannuelles établissant les priorités des années à venir, telles que le programme de Tampere, le programme de La Haye et récemment, le programme de Stockholm (qui se termine en 2014).

Cet objectif couvre un large éventail de politiques et de questions : la lutte contre la discrimination, la coopération judiciaire et policière, l'application de la libre circulation, les politiques en matière d'asile et d'immigration, la lutte contre le terrorisme, etc.

En tant qu'outil de prévention et d'investigation permettant d'observer les mouvements à l'intérieur et aux frontières de l'espace Schengen, le SIS II représente un instrument complet et essentiel à l'accomplissement de cet objectif.

2.1.2. Qu'est-ce que le SIS II : finalités du système

Divers organismes ont accès au SIS II : les autorités nationales chargées du contrôle des frontières, les autorités policières, douanières et judiciaires, les autorités chargées des visas et les services chargés de l'immatriculation des véhicules, ainsi que les agences européennes telles qu'Europol et Eurojust. L'agence internationale INTERPOL y aura également accès dès qu'un accord avec l'UE aura été trouvé. Le SIS II est une base de données centrale dans laquelle des « alertes » concernant des personnes et des objets sont enregistrées par les autorités compétentes des États membres aux fins décrites dans la convention de Schengen.

Lorsqu'un un ressortissant d'un pays tiers entre dans l'espace Schengen ou dépose une demande de visa auprès d'une ambassade ou d'un consulat européen, une recherche est lancée dans le SIS II afin de s'assurer que le demandeur ne fait l'objet d'aucun signalement. Si aucune alerte n'a été faite et si le demandeur répond à tous les autres critères requis pour l'obtention d'un visa, alors l'autorité compétente peut le lui délivrer. Si, au contraire, le demandeur fait l'objet d'un signalement, alors sa demande est automatiquement refusée. Plus de la moitié des plaintes liées au SIS reçues par les autorités de protection des données concernent des ressortissants de pays tiers qui se sont vu refuser un visa. De telles alertes reposent sur des décisions nationales qui peuvent potentiellement ne pas être conformes aux conditions strictes prévues par la loi ou ne pas être dûment justifiées. Les normes nationales pour émettre un signalement dans le SIS II peuvent également varier d'un État membre à l'autre, ce qui révèle un manque d'harmonisation. Ces divers aspects font du SIS II une base de données très risquée du point de vue de la protection des données et des risques de discrimination.

En ce qui concerne les objets, l'utilisation la plus courante du système est le signalement de véhicules volés. Par exemple, si une voiture est volée dans un État membre, ses données font l'objet d'un signalement dans SIS II de sorte qu'elles puissent être vérifiées lors des contrôles à l'entrée et à la sortie de l'espace Schengen.

16. L'Agence EUROPOL (« European Police Office ») créée par la Convention EUROPOL de 1995 remplacée depuis par la Décision du Conseil 2009/371/JAI est l'agence européenne de maintien de l'ordre, qui assiste les États Membres dans leurs investigations internationales.
17. EUROJUST (European Union's Judical Cooperation Unit) créée par la Décision du Conseil 2002/187/JAI qui a été amendée en 2009 par la Décision du Conseil 2009/426/JAI est l'agence européenne en charge de la coopération judiciaire en matière pénale et qui assiste les États Membres en ce sens.

Cependant, SIS II est également devenu – du fait de sa mise à jour - un outil d'appui aux enquêtes menées par les autorités nationales et européennes d'application de la loi. Considérant à la fois l'augmentation du volume d'informations qui peut légalement être traité par le système et l'augmentation du nombre d'acteurs y ayant accès, cette nouvelle fonction transforme SIS II en un outil d'investigation et d'échange d'informations à risques.

2.1.3. Le régime juridique du SIS II

2.1.3.1 Les textes mettant en œuvre le SIS II

La première version du SIS reposait sur les deux instruments des« Accords Schengen » du 19 juillet 1999, à savoir « l'Accord Schengen sur l'abolition graduelle des contrôles aux frontières communes » et la « Convention sur l'application de l'Accord Schengen ». Pour s'adapter aux évolutions de la construction européenne, ces accords ont été transformés par des textes législatifs européens.

SIS II est désormais mis en œuvre selon trois textes législatifs, qui gouvernent différents domaines d'activité du système : La Décision du Conseil 2007/533/JAI[18] dans le cadre de la coopération policière et judiciaire ; le Règlement n°1987/2006[19] du Parlement européen et du Conseil pour les questions de visas, d'asile, d'immigration et toute autre politique en lien avec la liberté de circulation des personnes ; et le Règlement n°1986/2006[20] du Parlement Européen et du Conseil concernant les acteurs délivrant des certificats d'immatriculation de voitures.

2.1.3.2. Les textes régissant la protection des données

En ce qui concerne les données traitées dans le système SIS II, la Convention 108 du CdE, et la Recommandation 87 du CdE sur le traitement des données personnelles dans le secteur policier donnent la base juridique de protection. La Directive 95/46/CE ne s'appliquant que sur les traitements émanant du droit communautaire, elle n'est prise en considération que par rapport au statut d'indépendance des autorités de contrôle qui sont investies de compétences de contrôle sur la partie nationale du SIS II (le N-SIS) dans chaque État membre.

2.1.3.3. Les textes portant sur l'implication de certains acteurs

Le corpus législatif de SIS II renvoie aussi vers les législations européennes instituant les agences EU-LISA[21], EUROPOL et EUROJUST pour en souligner certains aspects dans leurs activités avec SIS II.

---

18. Décision 2007/533/JAIdu Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)
19. Le 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)
20. Le Règlement (CE) n°1986/2006 du 20 décembre 2006 sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II)
21. Le règlement n° 1077/2011 du Parlement européen et du Conseil de l'UE établissant l'Agence européenne EU-LISA. Cette agence a pour but de gérer opérationnellement SIS II, mais aussi VIS (le système d'information pour les visas) et EURODAC (la base de données pour les demandes d'asile, de protection internationale et sur les immigrés traversant les frontières illégalement). EU-LISA a son siège à Tallin (Estonie), ses opérations se font à Strasbourg (France) et un ordinateur de sauvegarde se trouve à Sankt Johan Im Pongau (Autriche). Le nom complet de EU-LISA est en anglais "European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice"

2.2. Portée de SIS II

2.2.1. Impact sur les citoyens : la mobilité et l'entrée dans l'UE

SIS II qui était au début un outil de recherche de personnes et d'objets pour la prévention du crime transfrontalier et la protection des frontières externes de l'espace Schengen, est devenu, surtout par l'usage fait par les autorités policières, un moyen d'exclusion. Il apparaît que le principe de la libre circulation à l'intérieur de l'espace Schengen ne s'applique que pour les ressortissants des États membres. L'entrée dans l'UE des citoyens des États tiers est soumise à de très fortes limitations et à un très fort contrôle. Ces limitations sont encore plus strictes pour les personnes en situation difficile, comme les immigrés, les demandeurs d'asile, dont les données personnelles sont souvent entrées dans le système, sans qu'ils aient les moyens de vérifier ou de corriger la conformité de ces signalements avec les principes de légitimité et de proportionnalité. Le système a donc un impact important sur le droit des personnes de circuler librement.

2.2.2. Les données collectées

Suite à la mise à niveau de SIS II, le nombre et le type de données collectées ont été fortement augmentés. Il existe deux catégories de données (subdivisées en sous-catégories). Elles portent sur les personnes et sur les objets.

2.2.2.1. Les signalements sur les individus

SIS II contient des signalements sur les catégories d'individus (ressortissants ou pas de l'Union européenne) :

• les personnes recherchées pour être arrêtées à des fins d'extradition ou de remise aux autorités qui ont délivré un mandat d'arrêt européen

• les personnes disparues

• les personnes recherchées devant participer à une procédure judiciaire (qu'elles soient témoins, suspectées ou jugées)

• les personnes sujettes à des surveillances discrètes ou des contrôles spécifiques

Concernant ces individus les données suivantes peuvent être collectées :

• **Données personnelles :** les nom(s) et prénom(s), nom(s) de naissance, noms utilisés antérieurement et pseudonymes, le lieu et la date de naissance, le sexe ;

• **Données physiques :** des signes particuliers, objectifs et inaltérables

• **Données biométriques :** les photographies et les empreintes digitales ;

• **Données contextuelles :** l'indication que la personne concernée est armée, violente ou en fuite ;

• **Conditions du signalement :** le nom de l'autorité qui a signalé ; le motif du signalement ; une référence à la décision qui est à l'origine du signalement ; le(s) lien(s) vers d'autres signalements introduits dans le SIS II, le type d'infraction, les mesures à prendre.

2.2.2.2. Les signalements sur les objets

Pour les **objets**, le signalement a pour fins :

• La surveillance discrète ou des contrôles spécifiques. Cela inclut des véhicules, des embarcations, des aéronefs ou des conteneurs

• La saisie ou l'usage en tant que preuve dans le cadre d'une procédure pénale. Celles-ci comprennent entres autres des véhicules à moteur, des remorques, des armes à feu, des documents officiels vierges, des documents d'identité, des certificats et plaques d'immatriculation, des billets de banque et des titres et moyens de paiement[22].

2.2.2.3. Autres données échangées

D'autres données dont l'usage est conditionnel peuvent être échangées. Elles concernent :

• Pour les personnes recherchées à des fins de remises, le mandat d'arrêt européen

• Dans les cas d'usurpation possible d'identité, la victime doit aussi délivrer ses données qui sont usurpées (ex : détails personnels, information sur l'apparence, biométrie…).

En outre les Bureaux SIRENE, qui sont les liaisons de chaque État participant collectent leurs propres informations supplémentaires qui peuvent être de nature à servir l'action.

2.2.2.4. Durée de conservation des données

La durée de conservation des signalements diffère selon le signalement.

Concernant les **signalements sur les personnes**, le principe de protection des données est appliqué, selon lequel les signalements ne sont conservés que le temps nécessaire à la réalisation de l'objectif. A titre d'exemple, une personne retrouvée ne devrait plus être signalée dans SIS II.

Par conséquent, trois ans après l'entrée d'un **signalement sur une personne** recherchée, les États participants doivent examiner la nécessité de conserver ce signalement. Pour les surveillances discrètes ou les contrôles spécifiques, l'examen se fera au maximum un an après l'entrée du signalement.

Au cas où l'extension de la durée de conservation est jugée nécessaire, la décision doit être justifiée par les États participants qui doivent aussi suivre statistiquement ces demandes d'extension. Sans réponse de l'État signalant, à la fin de la durée de l'examen, le signalement est automatiquement supprimé.

Toutefois, les législations de SIS II n'énoncent pas concrètement de durée limite pour la conservation des signalements. Il est cependant mentionné qu'elles doivent être « courtes » et dépendent des législations nationales. Quatre mois avant la fin indiquée de conservation d'un signalement, la base de données centrale de SIS II (« CS-SIS ») alerte l'État afin qu'il évalue et indique s'il souhaite conserver le signalement.

Pour les objets ayant pour finalité d'être saisis ou utilisés en tant que preuve dans une procédure pénale, la conservation est de 10 ans, pour ceux surveillés discrètement et sujets à des contrôles spéciaux, la durée de conservation est de 5 ans.

Concernant les **données personnelles** échangées en tant qu'informations supplémentaires par les bureaux nationaux SIRENE, elles sont conservées le temps nécessaire à la réalisation de l'objectif. Autrement elles doivent être supprimées au maximum un an après le signalement de la personne concernée. Toutefois, les États peuvent garder ces informations, dans leurs fichiers nationaux. Dans ces cas, le temps de conservation qui s'applique est celui découlant de la législation nationale.

---

22. Décision du Conseil 2007/533/JAI, Article 38 (2) : *« a) les véhicules à moteur d'une cylindrée supérieure à 50 cm3, les embarcations et les aéronefs; b) les remorques d'un poids à vide supérieur à750 kg, les caravanes, le matériel industriel, les moteurs hors-bord et les conteneurs; c) les armes à feu; d) les documents officiels vierges volés, détournés ou égarés; e) les documents d'identité tels que passeports, cartes d'identité, permis de conduire, titres de séjour et documents de voyage délivrés qui ont été volés, détournés, égarés ou invalidés; f) les certificats d'immatriculation et les plaques d'immatriculation volés, détournés, égarés ou invalidés; g) les billets de banque (billets enregistrés); h) les titres et les moyens de paiement tels que chèques, cartes de crédit, obligations et actions volés, détournés, égarés ou invalidés. »*

2.2.2.5. Capacités opérationnelles

Dans la version première de SIS, il y avait en janvier 2012, plus de 42 millions d'entrées dont :
• 40,8 millions concernaient des objets
• 1,2 millions concernaient des personnes

Parmi les personnes, 692 000 entrées concernaient des étrangers « indésirables »[23].

Dans le SIS II, il y a environ 45 millions de signalements dont :
• 39 millions concernent des documents perdus ou volés
• 5 millions des voitures volées

Le SIS II a une capacité d'exploitation de 70 millions de signalements et, suivant les résultats des tests faits avant sa mise en œuvre, il peut aller jusqu'à 100 millions de signalements, sans qu'il y ait besoin de faire évoluer sa technologie[24]. SIS II a été pensé pour être un outil flexible…

2.3. Fonctionnement de SIS II

2.3.1. L'architecture technique

SIS II est composée de :
• un système central (SIS II Central) composé lui-même de la base centrale de SIS II et une interface nationale uniforme (NI-SIS) pour chaque État participant.
• **les sections nationales :** chaque État participant possède une base de données nationale (le N.SIS II) qui nourrit la base centrale par le biais de l'interface NI-SIS. Le N.SIS II contient une « copie nationale » complète ou partielle de la base de données du SIS II qui sert à l'interrogation sur le territoire national du contenu de SIS II Central.
• **l'infrastructure de communication** raccorde le CS-SIS aux différents NI-SIS et offre un réseau virtuel crypté pour les échanges entre les différents éléments de SIS II et les échanges entre les Bureaux SIRENE.

Les fichiers nationaux contenus dans chaque N.SIS II ne sont pas accessibles directement par les autres États participants. Pour obtenir des données, il faut impérativement passer par le SIS II Central, en y effectuant une recherche. Si elle en ressort positive, l'autorité chercheuse prend contact avec l'autorité nationale qui a entré le signalement.

2.3.2. Les procédures opérationnelles

Les acteurs responsables de l'opérationnel

Au niveau national, les bureaux N.SIS II de chaque État participant transmettent les « alertes » au SIS II Central. Ils sont aussi en charge de l'opérationnalité et de la sécurité du N-SIS II. Pour cela ils s'assurent que les autorités compétentes aient accès au SIS II tout en prenant les mesures nécessaires à ce que les dispositions établies dans les textes de loi soient bien suivies par tous les acteurs nationaux. Ces bureaux sont bien souvent localisés dans les services de Police ou du ministère de l'Intérieur. Dans de nombreux États, c'est le service informatique ou information-communication de la Police qui est en charge du N.SIS II[25].

23. Source: Council of the EU (2012), Note from the French Delegation – Document 8281/12, 28 March 2012
24. Source: European Commission Memo Questions and Answers: Schengen Information System (SIS II) 9 April 2013
25. Liste des offices N.SIS II et des bureaux SIRENE nationaux : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:103:0117:0124:EN:PDF

Les **Bureaux SIRENE** ont pour rôle de fournir les informations supplémentaires, liées aux signalements, aux autorités les requérant et de vérifier la qualité des informations entrées dans le SIS II - y ayant donc un accès complet.

Chaque signalement entré est sous la responsabilité de l'autorité qui l'a soumis.

Au niveau européen, l'agence **EU-LISA** est responsable de la gestion opérationnelle des grands systèmes d'information SIS II, VIS et EURODAC. Elle est entre autres chargée d'adopter et de mettre en œuvre des mesures de sécurité, de s'assurer de la séparation des données entre les trois systèmes et d'assurer le respect de la protection des données.

2.3.2.1. Les différents acteurs ayant des droits d'accès, complet ou partiel, au SIS II

Le droit de consulter SIS II diffère selon les acteurs.

Les acteurs qui ont un accès complet sont :

• Pour le contrôle aux frontières, les autorités responsables de l'identification des ressortissants de pays tiers.

• Dans les États membres, les autorités policières, douanières et judiciaires désignées par les États participants.

Les acteurs qui ont accès partiellement au SIS II et qui n'ont accès qu'aux informations nécessaires à l'exercice de leurs fonctions sont :

• Pour les données sur l'immigration : les autorités en charge de délivrer des visas (ambassades/ consulats) et les autorités centrales d'immigration.

• Pour vérifier les plaques d'immatriculation et tout élément en lien avec la déclaration d'un véhicule : les autorités d'enregistrement des véhicules.

• EUROPOL, pour les signalements en lien avec des arrestations, des surveillances discrètes ou des contrôles spécifiques, ainsi que pour les objets devant être saisis ou utilisés en tant que preuve dans une affaire criminelle.

• EUROJUST, pour les signalements en lien avec des arrestations et des affaires judiciaires.

Si un accord est trouvé entre l'Union Européenne et INTERPOL, ce dernier pourrait avoir un accès partiel au SIS II portant sur les données des passeports volés, détournés, égarés ou invalidés. Pour que cet accord se fasse, l'Union européenne exige d'INTERPOL et des pays qui ont délégué des membres à l'agence internationale qu'ils aient un niveau adéquat de protection des données et de respect des libertés fondamentales. Dans tous les cas, toute transmission ne pourrait se faire sans l'aval de l'État européen qui a émis le signalement. En retour, les États européens devraient avoir un accès direct aux données contenues dans la base de données d'INTERPOL sur les documents de voyage volés ou manquant.

2.3.2.2. Sécurité des données : les garanties

2.3.2.2.1. Mesures de sécurité générale

Les États participants, incluant les Bureaux SIRENE, ainsi que l'Autorité européenne de Gestion EU-LISA, doivent assurer la sécurité générale du système, ce qui comprend entre autres la protection de l'infrastructure, le contrôle des personnes qui accèdent aux données (registres), la gestion des données (accès, utilisation, transmission…) et l'évaluation du système (audit). Toutes les personnes travaillant sur SIS II sont liées par le secret professionnel.

Les États membres ont une responsabilité légale en cas de violation des droits des personnes. Ils ont la responsabilité d'imposer des sanctions en cas d'usage frauduleux de SIS II ou d'échanges illégaux d'informations supplémentaires.

Chaque interconnexion de signalements doit respecter les conditions émises pour chaque signalement.

Tous les deux ans EU-LISA délivre un rapport aux institutions européennes sur le fonctionnement technique de SIS II et sur l'infrastructure de communication, incluant les échanges supplémentaires qu'elle transmet. Tous les quatre ans la Commission européenne effectue une évaluation générale du SIS II et des échanges supplémentaires.

Les données traitées ne peuvent être réutilisées à d'autres fins administratives.

La surveillance conjointe de SIS II est assurée par l'Autorité commune de contrôle Schengen (JSA Schengen) qui adopte des opinions sur des questions relatives à la protection des données personnelles. L'Autorité commune examine les problèmes d'interprétation ou tout ce qui entrave l'application des textes législatifs, et de façon générale, toutes difficultés amenant l'exercice des droits des personnes. Elle formule aussi des propositions pour répondre aux problèmes rencontrés.

Cette coopération implique aussi de mener des audits et des inspections.

2.3.2.2.2. Surveillance des accès au SIS II

Au vu du nombre important d'acteurs pouvant consulter le SIS II, plusieurs procédures sont inscrites dans les textes législatifs afin de surveiller les accès de ces différents acteurs :

- Enregistrement des accès par les autorités nationales mais aussi par EUROJUST et par EUROPOL
- Mise à jour permanente des listes des personnes ayant accès au SIS II
- Contrôle des transmissions afin de vérifier quel acteur a le droit de recevoir des données personnelles
- Contrôle de l'introduction afin de vérifier quelles données personnelles ont été entrées, quand, par qui et pour quelles finalités.

Ces procédures s'appliquent aussi à EUROJUST et EUROPOL.

2.4. SIS II : Difficultés et risques

2.4.1. Difficultés

SIS II est fondé sur une législation très complexe, difficilement maîtrisable, construite sur un schéma dépassé des compétences de l'Union européenne.

2.4.2. Risques

Une technologie sous contrôle ?

Au vu des capacités opérationnelles actuelles et attendues de SIS II, le système requiert une technologie assez puissante. Le piratage du N.SIS II danois[26] moins de 2 mois après sa mise en œuvre opérationnelle et les sept ans de retard opérationnel de SIS II, amène à se demander si sa technologie est réellement maîtrisée, tant au niveau national qu'européen et du point de vue de la sécurité.

Les risques d'un outil flexible guidé par une approche sécuritaire

SIS et SIS II ont été façonnés afin de répondre aux besoins de sécurité des États membres dans la continuité de la politique Schengen, besoins renforcés au prétexte des attaques terroristes du 11 septembre 2001.

Depuis, des acteurs tels que EUROPOL, EUROJUST voire INTERPOL, ont été ajoutés au système. Bien que leur présence crée davantage de craintes, sur le principe, qu'il n'y ait à l'heure actuelle de preuves concrètes de leur danger, le système opérant à peine, le Contrôleur Européen à la Protection des Données et l'Autorité Commune de Contrôle Schengen, critiquent leur présence, ou du moins le manque de justification et de clarification de leurs rôles.

Conçu comme un outil de recherche, il est à craindre que SIS II ne dérive vers un outil d'investigation. La masse d'informations contenue dans SIS, augmentée avec SIS II, et l'introduction de données biométriques fait de lui le plus important système d'information de l'Union européenne. Si les données introduites ne sont pas suffisamment protégées et les acteurs suffisamment contrôlés, les répercussions peuvent être très graves pour les individus concernés. De plus, la législation de SIS II inclut l'usage « dès que possible » des empreintes comme éléments uniques d'identification[27] et non complémentaires à d'autres éléments, alors que de nombreux experts ont souligné le manque de fiabilité de ce type de données. Par ailleurs, les textes ne fournissent aucune disposition sur les mesures alternatives à prendre en cas d'incapacité à donner ses empreintes digitales.

Les limites des textes législatifs

Le droit d'accès à ses données par un individu est régi par le droit national et peut être direct ou indirect. En cas d'accès indirect au SIS II, aucun délai n'existe - pour les autorités des États participants ayant entré un signalement - pour informer un ressortissant de pays tiers de sa présence dans le SIS II ou pour en informer l'Autorité nationale de Contrôle de Protection des Données. En pratique, l'individu concerné découvre cette information, lorsqu'elle/il tente d'entrer légalement dans l'espace Schengen, ou au moment où une demande de visa lui est refusée. L'Autorité de Contrôle nationale, elle, découvre cette information si une plainte est émise par ce même individu.

---

26. Information relayée par la newsletter de juin 2013 du Contrôleur Européen à la Protection des Données.
27. Décision du Conseil 2007/533/JAI Article 2 (c) et Règlement 1987/2006 Article 22 (c): "as soon as this becomes technically possible, fingerprints may also be used to identify a person on the basis of his biometric identifier."

Ces manques nuisent gravement à la mobilité des ressortissants de pays tiers qui sont d'autant plus discriminés que leur droit de recours est affaibli. En effet, ne pouvant se rendre dans l'Espace Schengen, ils ne peuvent pas se défendre directement.

2.

3. SYSTÈME D'INFORMATION DES VISAS (VIS)

3.1. La politique commune des visas couplée à la lutte contre le terrorisme

Dans l'optique de la libre circulation au sein de l'Espace Schengen, l'Union européenne a mis en place une **politique commune des visas** de manière à éviter le phénomène de « forum shopping » soit, un ressortissant de pays tiers s'étant vu refuser un visa par un des États Schengen faisant alors une demande auprès d'un autre État de l'Espace Schengen. Cette politique porte sur les visas à courts termes, donc ceux ayant une durée de validité maximum de 3 mois utilisables dans une période de 6 mois à partir de leur date de délivrance ainsi que les visas de transit à travers le territoire ou la zone de transit aéroportuaire. Au-delà, les États membres sont seuls à décider de leur politique d'attribution de visas. Cette politique repose sur cinq éléments dont VIS, qui est la base de données permettant aux États Schengen d'échanger des données (ex : photographie, empreintes digitales, nom) sur les demandeurs de visa. En outre, VIS s'intègre aussi à la politique du **Programme de Stockholm** en vue de renforcer le système des contrôles aux frontières extérieures. Il est aussi utilisé dans le cadre de **la lutte contre le terrorisme** ce qui explique le droit d'accès par les autorités répressives et EUROPOL aux données conservées dans le VIS si cela peut contribuer substantiellement à la prévention ou détection d'actions terroristes[28]. Enfin, VIS et particulièrement EURODAC font partis des éléments permettant la mise en œuvre du **Règlement Dublin III** qui a pour but de désigner l'État responsable de l'examen d'une demande d'asile. Dans le cas de VIS, un État qui aurait remis un visa à un demandeur d'asile aurait la responsabilité d'examiner la demande d'asile de ce dernier. A cet effet les autorités nationales en charge des demandes d'asile peuvent consulter VIS. Au niveau européen c'est l'Agence EU-LISA qui s'occupe de la gestion opérationnelle de VIS (voir partie sur SIS II).

3.2. Finalités de VIS : sélection et contrôle des personnes entrant dans l'Espace Schengen

En enregistrant des informations sur les demandeurs de visas et en les rendant disponibles à tous les États Schengen et à EUROPOL, VIS a pour finalité concrète de contrôler les entrées dans l'espace Schengen ainsi que l'immigration en s'assurant que les personnes qui obtiendront des visas ne sont pas des personnes recherchées et/ou ne resteront pas dans l'Espace Schengen illégalement.

3.2.1. Utilisation de VIS à des fins d'octroi de visa et d'identification des personnes

VIS n'est pas seulement utilisé lors d'une demande de visa mais aussi pendant la période de validité du visa et lors de demandes ultérieures faites par un même individu.

Au moment de la demande de visa, l'autorité responsable des visas de l'État Schengen collectera les données du demandeur qui portent entre autre sur son identité (incluant des données biométriques) et son séjour (voir tableau ci-après pour les données collectées), ainsi que sur la personne physique ou morale invitant ou prenant en charge les frais de séjour du demandeur.

L'autorité crée un dossier de demande de visa sur VIS où l'ensemble des données du demandeur sera envoyé. Suite à cela, l'autorité vérifiera si le demandeur a fait une demande de visa dans les cinq ans précédents. Si une demande a été faite mais qu'elle n'a pas encore reçu de réponse, l'autorité renverra le demandeur vers l'État qui s'est chargé de sa demande pour ainsi éviter le « forum shopping ».

28. Règlement EC n° 767/2008, art 3

Si une demande a été faite et qu'elle a abouti, cette demande sera liée à la présente demande. Les résultats des demandes passées sont pris en considération pour les octrois futurs. Lier les dossiers devrait faciliter le travail de sélection des demandeurs, et donc de contrôle des entrées, des autorités compétentes. Les raisons d'un refus, d'un retrait de visa ou la réduction de la période de validité sont aussi inscrites dans VIS.

La majeure partie des plaintes reçues par le CEPD concernant VIS porte sur des visas non octroyés. Il est important de souligner que le refus une fois d'un visa ne signifie pas que ceux qui suivront seront automatiquement refusés. Chaque demande doit être évaluée en fonction des informations disponibles sur le moment.

En outre, lors de voyages de groupes, les dossiers individuels de chaque demandeur de visa sont automatiquement liés les uns aux autres. C'est aussi bien le cas pour des groupes où les individus se connaissent (familles ou amis) que pour ceux qui ne se connaitraient pas, par exemple lors de voyages organisés par des agences de voyage.

Ainsi, les autorités chargées des visas assurent à la fois les rôles de saisie, rectification et effacement des données. Le responsable du traitement des données appartient souvent à l'autorité chargée des visas mais peut toutefois être une autre autorité en fonction des États membres[29].

Si une demande a abouti positivement, VIS sera utilisé lors de contrôles tant à la frontière que dans l'Espace Schengen et les autorités nationales en charge de ces contrôles ont accès au VIS.

3.2.2. Dans la continuité des politiques sécuritaires européennes : l'usage à des fins répressives de VIS

Dans le cadre de la prévention et de la détection des infractions terroristes, d'autres infractions pénales graves ou pour les enquêtes en la matière, EUROPOL et les autorités nationales ont aussi un droit d'accès à VIS.

L'agence EUROPOL y accède à des fins de collecte et d'analyse d'informations et de renseignements pour la lutte contre le terrorisme, le trafic de stupéfiants et d'autres formes graves de la criminalité internationale. EUROPOL a obligation de rendre anonyme les données collectées de manière à ce qu'on ne puisse plus identifier les personnes. Pour consulter VIS, l'unité d'EUROPOL responsable va demander l'accord de l'État participant qui a saisi les données dans le système.

Pour ce qui est des autorités nationales, leur marge de manœuvre est plus grande. Elles peuvent mener leurs recherches en utilisant une diversité de données mentionnées dans la demande de visa, incluant l'usage des coordonnées de la personne ayant adressé une invitation et/ou susceptible de prendre en charge les frais de séjour du demandeur. En cas de recherche positive, elles ont accès aux autres données extraites du formulaire de demande et aux photographies. Pour accéder à VIS, elles doivent faire une demande auprès d'une autorité désignée par un État participant qui fait suivre la requête à l'autorité centrale nationale.

En comparaison avec EUROPOL, les autorités nationales ont un accès plus important à VIS. De nombreuses données leur sont accessibles, ce qui accroît la vulnérabilité de ces dernières et requiert d'autant plus de précaution de la part des autorités nationales et des autorités leur offrant cet accès afin d'éviter tout abus.

29. Liste des autorités compétentes dont le personnel dûment autorisé sera habilité à saisir, à modifier, à effacer ou à consulter des données dans le système d'information sur les visas (VIS) (2012/C 79/05), 17.03.2012. Document disponible ici : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:079:0005:0018:FR:PDF (page accédée le 14 Novembre 2013)

3.3. Capacités opérationnelles de VIS

Au moment de la rédaction de cette monographie[30], VIS n'a pas encore été déployé dans tous les pays du monde. Après avoir commencé ses opérations en octobre 2011, la base de données est désormais opérationnelle dans 11 régions sur les 23 prévues[31].

Lorsqu'il sera en pleine capacité, le système VIS deviendra la plus grande base de données biométriques du monde, contenant les 10 empreintes digitales, elle pourrait contenir les données de 70 millions de personnes faisant une demande de visa en 5 ans[32].

Il a été prévu que VIS traite 20 millions de demandes de visa par an provenant de 134 pays et qu'il y ait 100 000 actions faites par jour. Initialement, il était prévu que ces données proviendraient de 30 États qui ont à leur charge jusqu'à 3 500 postes consulaires et 12 000 utilisateurs finaux[33].

30. Novembre 2013
31. Le système a été lancé en Afrique du Nord, au Moyen Orient, dans les pays dits « du Golfe », en Afrique de l'Ouest et centrale, en Afrique du Sud et de l'Est, en Amérique du Sud mais aussi en Asie centrale, en Asie de l'Est et du Sud ainsi que sur les Territoires Palestiniens occupés. Le 30 Septembre 2013, la Commission européenne a adopté une Décision déterminant le dernier ensemble de régions où VIS serait mis en œuvre. La dernière région concerne les États Schengen dans la mesure où VIS s'applique aussi aux demandes de visa aux frontières de ces États. Pour plus d'informations, voir : http://eeas.europa.eu/delegations/westbank/documents/news/20131107_faqonvis_en.pdf
32. Communiqué de Presse de la Commission Européenne « Visa Information System (VIS): The JHA-Council reaches a political agreement on the VIS Regulation and VIS Decision », Brussels, 12 June 2007.
http://europa.eu/rapid/press-release_IP-07-802_en.htm (page accédée le 14 Novembre 2013)
33. Fiche d'information de l'entreprise Daon, fournisseur de produits logiciels de vérification d'identité, sur le BMS de l'Union européenne, 2008.
http://www.nws-sa.com/biometrics/EU_Matching_CS.pdf (page accédée 14 Novembre 2013)

3.4. Données collectées et collecte des données : non-respect de certains principes et menaces sur la protection des données

<table>
<tr><td colspan="5">Données collectées au moment de la demande de visa</td></tr>
<tr><td colspan="4">Données du demandeur</td><td rowspan="2">Données de la personne invitant ou prenant en charge les frais de séjour</td></tr>
<tr><td colspan="2">Données identitaires</td><td>Informations sur le séjour et la demande</td></tr>
<tr><td>Données administratives</td><td>Données biométriques</td><td>Informations sur le séjour</td><td>Informations sur la demande</td><td>Personne physique</td><td>Personne morale</td></tr>
<tr><td>▪ nom, nom de naissance (incluant les noms antérieurs)
▪ prénom(s)
▪ sexe
▪ date, lieu et pays de naissance
▪ nationalité actuelle et à la naissance
▪ pour les mineurs: adresse, nom et prénom(s) du père et de la mère
▪ profession actuelle et employeur
▪ pour les étudiants: nom de l'établissement scolaire
▪ type et numéro du document de voyage avec le nom de l'autorité qui l'a délivré, la date de délivrance et d'expiration</td><td>▪ photographie numérisée
▪ 10 empreintes digitales*

*Exceptions au relevé :
• Enfants de moins de 12 ans
• Personnes en incapacité de les donner (ex : n'ayant pas de mains, mains qui tremblent, doigts abîmés…)
• Chefs d'État, membres de leur gouvernement et de leur délégation, lors d'invitations officielles</td><td>▪ destination principale,
▪ durée du séjour,
▪ but du voyage,
▪ dates prévues d'arrivée et de départ,
▪ première frontière d'entrée ou itinéraire prévu de transit</td><td>▪ numéro de la demande,
▪ lieu et date de la demande,
▪ type de visa demandé,
▪ l'indication qu'un visa a été demandé</td><td>▪ nom
▪ prénom
▪ adresse</td><td>▪ nom,
▪ adresse
▪ noms et prénoms d'une personne contact</td></tr>
</table>

Selon les cas de figures (refus, octroi, prolongation ou réduction du visa) des informations administratives sont ajoutées (ex : autorité ayant pris la décision). Que ce soit en cas de refus de la demande de visa, de retrait, d'annulation ou de réduction de sa validité, les raisons de cette décision sont indiquées. Il existe sept types de motifs de refus[34] qui vont de la falsification du document d'identité, à l'absence de moyens de subsistance suffisants pour retourner vers le pays d'origine. En outre, la présence d'un signalement dans SIS II pour non-admission entraîne le refus automatique de la demande de visa.

3.5. Des collectes de données disproportionnées et discriminantes

Le Groupe de Travail de l'Article 29 (Groupe 29) recommande de ne pas inclure les données des personnes invitant ou payant les frais de séjour des demandeurs de visa considérant que cela est disproportionné par rapport à la finalité de VIS. Si malgré tout il fallait les incorporer, elles devraient être consultables uniquement par les autorités centrales nationales en charge de délivrer des visas. Enfin, il s'oppose à ce que l'on demande à un individu sa nationalité de naissance pour éviter toute discrimination[35]. En outre, il demande à ce que soit défini précisément ce qu'est un « ressortissant de pays tiers » afin que soient exclus de VIS ceux qui ont obtenu un permis de séjour dans un État Schengen.

3.6. Conservation des données disproportionnée

Pour un séjour de trois mois maximum au sein de l'Espace Schengen, les demandeurs sont fichés avec toutes leurs données pendant cinq ans[36]. Au-delà de faciliter la procédure de demande de visa, il s'agit d'un réel contrôle des individus qui entrent au sein de l'Espace Schengen.

Pour éviter cette disproportion, le Groupe 29 a proposé d'établir un tableau de référence échelonnant les durées de conservation en fonction des résultats des demandes et de ses différents éléments[37]. A titre d'exemple, la conservation serait plus courte pour un visa refusé pour des raisons administratives (ex : absence de documents de voyages, de moyens suffisants de subsistance) et donc peu graves, et une durée plus longue pour un visa refusé pour des raisons qui porteraient sur des causes criminelles. Parmi leurs références, le Groupe 29 propose ainsi des durées de conservation de quelques semaines ou mois dans le premier cas, la suppression automatique de la demande pour des raisons de santé publique dès que le problème est résolu, la suppression automatique des liens entre les dossiers de demande lors de voyage de groupe dès que le visa a expiré. Si le refus d'un visa fait suite à un signalement dans SIS II, il est demandé que la durée de conservation dans VIS coïncide avec celle de SIS II.

3.7. Dix empreintes et l'impossibilité de s'opposer à leur collecte

Il est disproportionné de demander 10 empreintes digitales pour une demande de visa de trois mois, qui est conservée pendant cinq ans, et dont la finalité de la collecte est avant tout, de pouvoir identifier ou vérifier l'identité du demandeur ou du porteur de visa. Demander 10 empreintes c'est considérer la personne comme étant un criminel potentiel.

La quantité est d'autant plus importante que les seuls à ne pas pouvoir donner d'empreintes sont ceux qui ne peuvent physiquement pas le faire ou ceux dont la fiabilité est mise en question (ex : enfants de moins de 12 ans). Ainsi, si un individu refuse de donner ses empreintes, sa demande de visa n'est automatiquement pas traitée. Il n'y a aucune échappatoire possible.

34. Voir Article 12 Règlement n°768/2008
35. Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final), Adopted on 23 June 2005, ARTICLE 29 Data Protection Working Party
36. La date de début de conservation diffère selon les cas de figure. Voir Article 23 Règlement n°768/2008.
37. Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final), Adopted on 23 June 2005, ARTICLE 29 Data Protection Working Party

3.8. Une collecte des données pouvant nuire à la protection des données

La collecte des données biométriques peut se faire en dehors des locaux des ambassades et consulats Schengen, de plus, il est possible d'externaliser ce service. Utiliser ce type de service doit être exceptionnel, dûment justifié et les termes du contrat doivent être précis et inclure entre autre des clauses de confidentialité, de conformité avec la protection des données. Malgré toutes ces précautions, permettre une telle procédure c'est exposer un peu plus encore les demandeurs de visa, en particulier de détournement de leurs données personnelles. Cela est d'autant plus dangereux dans des pays perçus comme non démocratiques et dans les pays où le risque de corruption est grand. Plus spécifiquement pour ces pays qui ne sont pas soumis aux mêmes règles de protection des données, ce genre de délégation de service devrait être interdit, car cela peut nuire à la vie privée d'un individu, voire à mettre sa vie en danger (ex : le prestataire peut ainsi informer des tiers, des autorités, qu'une personne fait une demande de visa).

3.9. Droits des personnes au regard de VIS

Les droits des citoyens sont précisés dans le chapitre VI du règlement n° 767/2008/CE du Parlement Européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).

3.9.1. Droit à l'information

Au moment de la collecte des données du formulaire de demande, des photographies et des empreintes digitales, l'État Schengen responsable de cette collecte fournit les informations suivantes aux demandeurs et ce, par écrit :

• l'identité du responsable du traitement qui est l'autorité de contrôle nationale ainsi que ses coordonnées ;

• les finalités du traitement des données dans le VIS ;

• les groupes de destinataires de ces données incluant les autorités nationales de répression en charge de la prévention, de la détection et de l'investigation des infractions terroristes et autres infractions pénales graves ;

• la durée de conservation des données ;

• que la collecte des données est obligatoire pour l'examen de la demande ;

• **qu'ils ont des droits au regard du traitement de leurs données** : le droit d'accéder à leurs données, qu'elles soient rectifiées si elles sont erronées, supprimées si elles ont été traitées illicitement, le droit d'obtenir des informations sur les procédures à suivre pour exercer ces droits et les coordonnées des autorités nationales de protection des données qui peuvent être saisies en cas de réclamations relatives à la protection des données à caractère personnel.

Ces informations sont aussi à transmettre aux personnes invitant les demandeurs ou prenant en charge leurs frais de séjour et ce, par le biais du (des) formulaire(s) qu'ils ont à remplir et à signer. S'il n'y a pas de formulaires car les données ne sont pas collectées directement auprès d'elles, le responsable du traitement, doit les informer dès l'enregistrement des données ou, si une communication des données à un tiers est envisagée, au plus tard lors de la première communication de ces données.

3.9.2. Procédures des droits d'accès, de rectification, d'effacement et de recours

Chaque personne a le droit d'accéder aux données qui la concernent enregistrées dans le VIS ainsi que de connaître l'identité de l'État Schengen qui les a transmises. L'individu doit pouvoir exercer ce droit sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs. Cet accès peut être accordé par un État Schengen, n'importe lequel.

Pour la rectification et l'effacement des données, une personne peut s'adresser à n'importe quel État Schengen. Toutefois, c'est l'État Schengen responsable du traitement de la demande de visa qui doit

rectifier ou supprimer ces données. L'État que la personne a contacté pour exercer son droit d'accès devra prendre contact dans un délai de 14 jours avec l'État qui a traité la demande de visa et a enregistré des données, celui-ci a un mois pour vérifier l'exactitude de ces données. Les modalités de la vérification se font en fonction de la législation nationale.

Selon les cas de figure :

s'il y a bien eu erreur ou traitement illicite des données, l'État responsable les corrige ou les efface immédiatement et le confirme par écrit et sans délai à la personne concernée

S'il n'y a pas eu erreur ou traitement illicite des données, l'État responsable, l'indique par écrit et sans délai à la personne concernée en justifiant pourquoi il ne peut pas le faire.

En lien avec le deuxième cas, l'État responsable doit aussi informer la personne des recours possibles qu'elle a pour contrer cette décision. Cela comprend des informations sur les recours disponibles au niveau national, le dépôt d'une plainte devant les autorités compétentes ou les juridictions de l'État en question ainsi que sur les aides possibles des Autorités nationales de Protection des Données.

Toute demande, qu'elle soit d'accès, de rectification ou de suppression des données, doit être enregistrée par l'État Schengen responsable de l'exercice de ce droit.

L'Union européenne a lancé une campagne d'information sur VIS l'année de sa mise en œuvre dans les premiers pays tiers visés[38].

3.

38. Les éléments de cette campagne sont disponibles ici en français, anglais et allemand (page accédée 22/11/2013): http://ec.europa.eu/dgs/home-affairs/e-library/multimedia/publications/index_en.htm#0801262489da9f79/c_

4. "EUROPEAN DACTYLOSCOPY" OU EURODAC

Note : la présentation ci-après se base sur la nouvelle législation adoptée en juin 2013 et dont la mise en œuvre est prévue pour juillet 2015.

Les individus qui verront leurs données entrées dans EURODAC sont les demandeurs d'asile auprès d'un État membre de l'UE (dites « personnes demandant une protection internationale »), les ressortissants de pays tiers ou les apatrides qui ont été trouvés traversant illégalement une frontière extérieure de l'espace couvert par EURODAC ou ceux trouvés séjournant illégalement sur cet espace. Par ailleurs, les règles d'EURODAC s'appliquent aux États Schengen membres et non-membres de l'UE[39]. Toutefois, le Danemark n'y participe pas alors qu'il participe à la politique Schengen et inversement le Royaume-Uni et Chypre, qui ne sont pas des États Schengen, y participent.

Au niveau européen, l'acteur principal est EU-LISA (voir partie SIS II), et à la différence de SIS II et VIS, EURODAC n'est pas composé de systèmes nationaux reliés à la base de données centrale ; il n'y a donc qu'un fichier central.

En Décembre 2009, il y avait au total **1 544 558 entrées**[40] dans l'ancienne version d'EURODAC soit :
- 1 454 315 entrées relatives aux demandeurs de protection internationale[41]
- 90 243 entrées de personnes appréhendées à la frontière extérieure d'un État participant[42]
- 42 053 personnes séjournant illégalement sur le territoire couvert par EURODAC[43]

4.1. Lien avec les politiques de l'UE : De la politique Schengen au Programme de Stockholm, d'un outil pour l'application du Règlement Dublin III à un outil mis à la disposition des autorités répressives.

La politique Schengen qui a abouti à l'abolition des frontières intérieures dans l'espace Schengen et à la création d'une frontière extérieure unique, a pour corollaire la coopération des États participants dans le cadre de la lutte contre l'immigration illégale et EURODAC contribue à cet objectif général. En lien direct avec la politique Schengen, EURODAC est aussi un élément du Régime d'Asile Européen Commun (RAEC), et dans ce cadre a pour but de faciliter l'application du **Règlement Dublin III** ou Règlement n°604/2013, qui permet de déterminer l'État participant responsable de l'examen d'une demande de protection internationale.

Par ailleurs, le **nouveau Règlement (UE) n°603/2013, définissant EURODAC** prévoit l'accès par les autorités répressives des états membres, ainsi que par EUROPOL, aux données conservées dans EURODAC pour effectuer une comparaison des données personnelles dans un but de prévention, de détection et d'investigation en lien avec des activités terroristes ou infractions criminelles graves. Si, à l'origine, EURODAC permettait aux États participants, et uniquement eux, d'échanger des informations dans le cadre d'une demande de protection internationale ou lorsqu'un ressortissant d'un État tiers était trouvé illégalement sur le territoire d'un État membre, la récente réforme d'EURODAC prévoit un nouveau rôle pour le système qui s'inscrit directement dans la mise en œuvre des programmes successifs

39. Au 25 novembre 2013, moment de l'écriture, il s'agit pour les États Membres de l'UE de l'Allemagne, l'Autriche, la Belgique, *le Danemark (ne participe pas à EURODAC),* l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Slovaquie, la Slovénie et la Suède. Pour les pays non Membres il s'agit de l'Islande, du Lichtenstein, de la Norvège et de la Suisse.
40. Source : Commission européenne, Rapport annuel au Parlement européen et au Conseil sur les activités de l'unité centrale d'Eurodac en 2009, COM/2010/0415final, du 2Août2010
41. Idem.
42. Idem.
43. Idem.

de la Haye et de Stockholm. **Le Programme de Stockholm** établit les nouvelles priorités jusqu'en 2014 et met en avant une Europe « ouverte et sécurisée » où il serait nécessaire, dans le cadre d'activités répressives, que les États membres échangent entre eux des informations.

4.2. Finalités d'EURODAC

4.2.1. Déterminer l'État responsable d'une demande de protection internationale

Le rôle premier d'EURODAC est de déterminer quel État participant est responsable de l'examen d'une demande de protection internationale en application du Règlement Dublin III qui par des critères, ordonnés de façon hiérarchique, permet d'aboutir à cette finalité.

Les premiers critères cherchent à favoriser la réunification familiale. S'ils ne s'appliquent, il convient par la suite de vérifier si le demandeur a franchi irrégulièrement la frontière d'un État en venant d'un pays tiers, auquel cas cet État est responsable de l'examen de la demande de protection internationale (cette responsabilité prend néanmoins fin 12 mois après le franchissement irrégulier de la frontière). Par ailleurs, lorsqu'aucun État participant ne peut être désigné responsable sur la base des autres critères, le premier État auprès duquel la demande de protection internationale a été introduite est responsable de l'examen.

Ainsi, pour mettre en œuvre le Règlement Dublin III, EURODAC permet, en comparant les empreintes digitales, de vérifier si un demandeur de protection internationale ou un ressortissant étranger retrouvé illégalement sur le territoire d'un État participant a déjà formulé une demande dans un autre État participant, ainsi que de vérifier si un demandeur de protection internationale est entré irrégulièrement sur le territoire d'un des États participants. Ces vérifications permettent alors d'appliquer les règles correspondantes du Règlement Dublin III pour déterminer l'État responsable du traitement de la demande de protection internationale.

4.2.2. Contribuer à la lutte contre le terrorisme et aux infractions pénales graves : stigmatisation d'un groupe vulnérable

En vertu du nouveau Règlement, chaque État participant désignera une **autorité compétente en charge de la prévention, de la détection ou de l'investigation des infractions terroristes ou d'autres infractions pénales graves** qui sera autorisée à demander les comparaisons d'empreintes digitales avec les données d'EURODAC.

Toutefois, les autorités nationales et EUROPOL n'ont pas un accès illimité à EURODAC. Elles doivent faire une demande de consultation qui doit être justifiée et remplir toute une série de conditions. Ainsi, il faut par exemple qu'elles aient préalablement consulté et ce, sans succès, d'autres bases de données d'empreintes digitales pour déterminer l'identité d'une personne. La comparaison doit également être nécessaire dans un cas précis ; les recherches systématiques sont strictement interdites. A titre d'exemple, EUROPOL peut accéder à EURODAC lorsque l'agence veut comparer une empreinte digitale latente retrouvée sur une scène de crime.

Il faut également noter que les informations obtenues par EUROPOL à la suite de la comparaison avec les données d'EURODAC ne peuvent être traitées qu'avec l'autorisation de l'État membre qui a transmis les informations au système central.

Ce nouvel aspect d'EURODAC, soit l'accès rendu possible aux autorités répressives, a été fortement critiqué que ce soit par le CEPD, le Groupe de Travail de l'Article 29, le groupe de supervision de la Coordination d'EURODAC, et par le groupe de supervision d'EUROPOL, critiquant l'absence de preuves sur la nécessité de cette nouveauté.

En effet, permettre cet accès conduit à une stigmatisation des demandeurs de protection internationale, considérés comme de potentiels criminels, alors que ce groupe est a priori très vulnérable. En outre, le texte d'EURODAC ne mentionne pas quel type d'informations peut être partagé avec les autorités de répression lorsqu'il y a une correspondance d'empreintes digitales, suite à une recherche qu'elles ont effectuée.

4.3. Peu de données entrées, mais des données importantes : pour vérifier et amener des échanges a posteriori

Comme dit précédent, il existe trois catégories possibles d'individus dont les données seront conservées dans EURODAC. Pour les deux premières catégories, soit un individu qui a fait une demande de protection internationale et une personne retrouvée traversant illégalement une frontière extérieure, les données stockées diffèrent légèrement. **Il est important de noter que les empreintes digitales ne peuvent cependant pas être prises sur des personnes de moins de 14 ans.**

Les données pour les deux premières catégories de personnes se présentent de façon suivante :

Type de demandeurs	**Demandeur d'une protection internationale** *Collecte des données lors de la présentation d'une demande*	**Ressortissant d'un pays tiers ou apatride trouvé traversant illégalement une frontière extérieure**[1]
Les données personnelles enregistrées	- Les empreintes digitales des 10 doigts ou des index au minimum - Le sexe	- Les empreintes digitales des 10 doigts ou des index au minimum - Le sexe
Les données administratives enregistrées	- Le nom de l'État membre d'origine (soit l'État où la demande a été formulée), le lieu et la date de la demande de protection internationale[2] - Le numéro de référence utilisé par l'État membre d'origine quant à la demande - La date à laquelle les empreintes ont été relevées - La date à laquelle les données ont été transmises au système central; - Le code d'identification de l'opérateur	- Le nom de l'État membre d'origine (qui a entré les données), le lieu de l'interpellation et la date de la demande de protection internationale[3] - Le numéro de référence utilisé par l'État membre d'origine quant à la demande - La date à laquelle les empreintes ont été relevées - La date à laquelle les données ont été transmises au système central; - Le code d'identification de l'opérateur
Informations supplémentaires enregistrées	Les informations sur le statut du demandeur en lien avec sa demande, soit le cas échéant : - la date d'arrivée de l'intéressé, après un transfert. - la date à laquelle la personne concernée a quitté le territoire des États couverts par EURODAC pendant une durée d'au moins 3 mois. - la date à laquelle la personne concernée a été sujette à une décision de retour ou a été éloignée du territoire couvert par EURODAC ou l'a quitté suite à un retrait ou rejet de la demande. - la date à laquelle la décision d'examiner la demande a été prise.	Aucune autre information n'est enregistrée.
La durée de conservation	**Conservation pendant 10 ans** dans le système central. Passé le délai, effacement automatique par le système central.	**Conservations pendant 18 mois** dans le système central. Passé le délai, effacement automatique par le système central.
Les conditions d'effacement anticipées	Acquisition de la nationalité d'un des États participants. Le système central en informe dès que possible tous les États qui ont entrés les données.	La personne a obtenu un document de séjour, elle a quitté le territoire couvert par EURODAC, elle a acquis la nationalité d'un des États participants.

Précisions : A la différence, d'un demandeur de protection internationale, les données d'un ressortissant d'un pays tiers ou apatride, interpellé lors du franchissement irrégulier d'une frontière extérieure, ne font pas l'objet d'une comparaison automatique en vue de faciliter la détermination des critères relevant du Règlement Dublin III. Elles sont, en effet, enregistrées aux fins de leur comparaison ultérieure avec les données qui sont transmises au système central, dans le cadre d'une demande de protection internationale, dans le but alors, de faciliter la détermination des critères de Dublin III à appliquer pour déterminer l'État responsable de la demande (voir partie 4.2.1.). Ces données seront également comparées par les autorités répressives et EUROPOL lors d'une demande de comparaison de leur part.

Pour la troisième catégorie d'individus, soit **ceux qui sont interpelés** (par exemple dans un transport en commun) **et s'avèrent séjourner illégalement dans un des pays EURODAC**, seules les empreintes sont collectées et ce, **à titre de comparaison**, pour vérifier si une demande de protection internationale n'a pas été introduite auparavant dans un des États participants. Cela est particulièrement le cas si la personne déclare avoir introduit une demande de protection internationale mais n'indique pas auprès de quel pays elle l'a faite, si elle dit ne pas en avoir introduite mais qu'elle s'oppose au renvoi dans son pays car elle y serait en danger ou encore si elle essaie d'empêcher son renvoi vers un autre pays tiers en empêchant que son identité soit établie. Ces données **ne sont pas comparées** avec celles d'individus interpellés pour avoir traversé illégalement une frontière extérieure. Elles **ne sont pas conservées** dans EURODAC.

En outre, on constate qu'il y a assez peu de données personnelles échangées dans EURODAC en comparaison des autres systèmes présentés dans cette monographie, ce qui n'en réduit pas leur gravité. Cela s'explique par le fait qu'EURODAC est un système dactyloscopique qui contient donc principalement des empreintes digitales. Toutefois**, cela ne signifie pas que les autres données personnelles telles que le nom ou la nationalité ne sont pas conservées ni échangées**. Elles sont conservées dans des fichiers nationaux comme le démontre le numéro de référence présent dans EURODAC. En effet, pour pouvoir déterminer l'État responsable d'une demande de protection internationale, le Règlement Dublin III prévoit que les États échangent des données personnelles concernant les demandeurs. **L'échange de ces données prend la forme d'une coopération administrative** et sont échangées directement entre les États via un système d'emails sécurisés.

Utilisation par les États d'EURODAC

Une fois les empreintes collectées, les autorités compétentes doivent alors transmettre ces données à l'unité centrale d'EURODAC dans un bref délai et les empreintes digitales sont alors comparées automatiquement avec celles transmises par d'autres États membres antérieurement, qui sont déjà conservées dans le système.

Le système central transmet alors le résultat positif ou négatif de la comparaison à l'État membre à l'origine de la demande de comparaison.

Au cas où il n'existe aucune correspondance avec des empreintes déjà stockées dans EURODAC, l'unité centrale le fait savoir à l'État requérant et ne transmet pas d'information à l'État requérant.

Au cas où la comparaison débouche sur une correspondance des empreintes du demandeur de protection internationale avec des empreintes déjà stockées dans EURODAC, l'unité centrale transmet à l'État ayant requis la comparaison les données mentionnés dans le tableau ci-dessus.

Par ailleurs, les États ont accès uniquement aux données qu'ils transmettent dans EURODAC. Ils n'accèdent aux données des autres États que si les comparaisons qu'ils ont faites ont trouvé une correspondance dans le système. Les acteurs nationaux en charge de modifier ou effacer les données erronées devraient être les autorités responsables des demandes et de l'octroi de l'asile de l'État membre qui a entré les données.

4.4. Problème de proportionnalité

Lorsque le demandeur ressortissant d'un pays tiers dépose sa demande de protection internationale dans un État participant, ses dix empreintes digitales ainsi que certaines autres données sont collectées et enregistrées par les autorités nationales compétentes. Cependant, prendre 10 empreintes pour identifier une personne n'est pas proportionné à cette finalité. La prise des 10 empreintes combinée à la consultation possible par des autorités de répression et d'EUROPOL, revient à assimiler les demandeurs à de potentiels criminels.

4.5. Vide juridique et impossibilité de s'opposer à la collecte des empreintes

EURODAC étant strictement un système sur les empreintes digitales, la collecte de ces empreintes est obligatoire. Si une personne, temporairement, ne peut pas les donner, elles seront relevées « dès que possible ».

Il est précisé dans les textes que **l'impossibilité temporaire ou permanente de recueillir et/ou de transmettre des données dactyloscopiques,** soit pour des raisons telles qu'une qualité insuffisante des données pour effectuer une comparaison appropriée, des problèmes techniques ou des motifs de protection de la santé, soit du fait que la personne concernée est mise dans l'impossibilité ou dans l'incapacité de fournir des empreintes digitales en raison de circonstances hors de son contrôle, **ne devrait pas avoir d'incidence négative sur l'examen de la demande de protection internationale que cette personne a introduite**. Mais cette information n'est reprise dans aucun article du texte législatif d'EURODAC, uniquement dans le considérant 20[44]. Cette absence dans le corps du texte, soulignée par le groupe de supervision de la Coordination d'EURODAC démontre qu'il existe un certain vide juridique

44. REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the establishment of Eurodac 'for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), Recital 20

dans les textes d'EURODAC. On peut alors se demander, au vu du rôle d'EURODAC, si cette personne apparaîtra quand même dans le système et particulièrement, si sa demande sera quand même traitée ?

Par ailleurs, il est important de souligner que si un demandeur refuse de donner ses empreintes digitales, cela peut nuire à la crédibilité de la demande qui sera refusée. En effet, la personne sera perçue comme n'ayant pas fait suffisamment d'effort pour aider à établir sa véritable identité.

4.6. Risques liés au transfert de données vers des pays tiers

Si à partir d'une recherche il y a une correspondance dans EURODAC, **les données utilisées pour cette recherche peuvent être transférées à des pays tiers, sauf s'il y a des risques graves pouvant nuire au demandeur** (torture, traitements inhumains et dégradants ou toute autre violation des droits fondamentaux de la personne). On parle là de données qui ne sont pas conservées dans le système central d'EURODAC mais ont leur origine dans un État membre et sont communiquées entre États membres à la suite d'un résultat positif de comparaison avec le système central. Vu le caractère vague des termes «risques graves», ce type de transfert devrait être interdit pour éviter toute interprétation erronée.

4.7. Droits des citoyens dans le cadre d'EURODAC

Les droits des citoyens sont précisés à l'Article 29 du Règlement 603/2013.

Droit à l'information:

Toute personne qui aura ses données introduites dans EURODAC est informée :

- de l'identité du responsable du traitement de données soit la personne ou organisme qui définit l'objet et les moyens du traitement de données à caractère personnel et de son représentant, le cas échéant
- des raisons pour lesquelles ses données vont être traitées par EURODAC, y compris une description des objectifs du règlement Dublin III
- du fait que les États membres et Europol peuvent avoir accès à EURODAC à des fins répressives et des explications, sous une forme intelligible, dans un langage clair et simple, quant au fait que les États membres et EUROPOL peuvent avoir accès à EURODAC à des fins répressives;
- des destinataires des données
- de son droit d'accéder aux données
- de son droit de demander que des données inexactes la concernant soient rectifiées ou que des données la concernant qui ont fait l'objet d'un traitement illicite soient effacées
- de son droit d'être informée des procédures à suivre pour exercer ces droits

Ces informations doivent être données au moment où les empreintes digitales de la personne concernée sont relevées ou au plus tard au moment où les données concernant cette personne sont transmises au système central (particulièrement le cas pour ceux retrouvés illégalement sur le territoire d'un État participant). Elles doivent être données à l'écrit et dans une langue que la personne comprend. Pour les mineurs, les informations doivent être communiquées d'une manière adaptée à leur âge.

Droit d'accès aux données conservées dans le système:

- la personne concernée a le droit d'obtenir les données la concernant qui sont enregistrées dans le système central ainsi que de l'identité de l'État membre qui les a transmises au système central
- l'individu doit pouvoir exercer ce droit sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs
- ce droit d'accès peut être exercé dans chaque État participant (mais un seul État peut autoriser l'accès)

Droit de rectification et d'effacement:

- Toute personne concernée peut demander que les données erronées soient rectifiées ou que les données enregistrées de façon illicite soient effacées. La rectification et l'effacement sont effectués sans retard excessif par l'État membre qui a transmis les données
- S'il apparaît que des données enregistrées dans le système central sont matériellement erronées ou y ont été enregistrées de façon illicite, l'État membre qui les a transmises les rectifie ou les efface et confirme par écrit et sans délai excessif à la personne concernée qu'il a procédé à la rectification ou à l'effacement de données la concernant
- Si l'État concerné n'estime pas que c'est le cas, il doit indiquer par écrit et sans délai excessif à la personne concernée les raisons pour lesquelles il n'est pas disposé à rectifier ou effacer les données. Il doit aussi informer la personne sur la manière de former un recours ou, s'il y a lieu, de déposer une plainte devant les autorités compétentes ou les juridictions de cet État membre, ainsi que sur toute aide, financière ou autre, dont la personne concernée peut disposer

En outre, si une personne a fait une demande de protection internationale, elle a le droit d'être assistée par l'Autorité Nationale de Protection des Données (DPA) dans l'exercice de ses droits.

4.

5. SYSTÈME EUROPÉEN D'INFORMATION SUR LES CASIERS JUDICIAIRES (ECRIS)

5.1. Politiques européennes : liberté de circulation et renforcement de l'assistance mutuelle en matière criminelle

5.1.1. Liberté de circulation : des condamnations « mobiles »

Grâce à la liberté de circulation, les ressortissants de l'UE et les membres de leur famille peuvent circuler et vivre librement dans n'importe quel État membre, l'UE a donc décidé de rendre les condamnations, elles aussi, « mobiles ». Ainsi un citoyen européen ne peut effacer son historique judiciaire en traversant une frontière.

5.1.2. Assistance mutuelle en matière criminelle: systématiser les échanges

Il s'agit de coopération entre les autorités judiciaires des États pour collecter, par exemple, des informations et des preuves dans le cadre d'enquêtes pénales ou de procédures judiciaires. ECRIS est un nouvel outil pour une telle coopération qui quant à cette dernière n'est pas nouvelle. La première législation européenne sur l'échange d'information de casiers judiciaires est la Convention du Conseil de l'Europe sur l'entraide judiciaire en matière pénale de 1959, qui a été ratifiée par tous les États membres de l'Union européenne (UE). Au niveau de l'UE, ce texte a été complété par l'Acte du Conseil du 29 mai 2000 établissant la Convention sur l'entraide judiciaire en matière pénale entre États membres de l'UE[45].

ECRIS va plus loin que ces textes en ce qu'il établit une coopération régulière et systématique. Lorsqu'une autorité judiciaire d'un État demande des informations car elle doit rendre une décision de justice sur un ressortissant d'un autre État, ce dernier doit notifier les condamnations criminelles à l'État Membre demandeur dans un bref délai. .Il apparaît, dans les textes législatifs d'ECRIS, que l'État de nationalité du prévenu devra envoyer les informations sur toutes les condamnations de son ressortissant sans forcément faire un tri en fonction des besoins de l'autorité judiciaire qui a fait la demande. Ceci pose la question du respect du principe de proportionnalité.

5.1.3. Le Conseil européen de Tampere et les programmes de La Haye et de Stockholm : reconnaître les décisions judiciaires pénales sans les harmoniser

Les conclusions du Conseil européen de Tampere en 1999 ont rappelé que l'UE se veut un « espace de liberté, de sécurité et de justice », ce qui implique la création d'un espace sécurisé où les individus peuvent circuler librement. De manière plus spécifique à ECRIS, les conclusions de Tampere mentionnaient que les décisions judiciaires en matière pénale doivent être reconnues dans tous les États membres. Les programmes de la Haye et de Stockholm qui ont suivi ont continué à développer les priorités à mettre en œuvre pour parvenir à un espace sécurisé pour les citoyens, via une coopération judiciaire renforcée entre États membres. ECRIS est censé contribuer directement à la création de cet espace en renforçant l'échange d'informations extraites des casiers judiciaires entres les États membres de l'UE.

45. Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne

Cette reconnaissance ne remet pas en question la multiplicité des systèmes judiciaires. Basée sur la confiance mutuelle, il est présupposé que chaque État a un système acceptable et que les condamnations qui en découlent n'ont pas à être remises en question notamment, sur la définition des infractions, crimes, délits ou leurs durées d'inscriptions. Or, si l'on prend par exemple le cas de l'avortement qui peut être pénalisé dans certains états membre et pas dans d'autres, on peut envisager des cas de traitement inégal des citoyens européens[46]. Au lieu de résoudre ces inégalités, ECRIS va les faire perdurer et même donner lieu à des échanges abusifs.

5.1.4. La lutte contre le terrorisme : un danger pour les Droits fondamentaux

La Déclaration du Conseil européen pour combattre le terrorisme de 2004[47] fait de la lutte contre le terrorisme une des priorités et pour cela il a été décidé d'améliorer la qualité des échanges d'information sur les condamnations pénales. Le programme de la Haye reprend ce point en insistant sur l'intensification des échanges d'informations sur les casiers judiciaires, y compris l'échange d'informations sur la perte de certains droits suite à des condamnations pénales.

Lorsque l'on sait que la lutte contre le terrorisme déroge souvent aux règles minimales de protection des droits des individus, il est inquiétant de voir qu'ECRIS, qui concerne une multiplicité de personnes, s'inscrit dans ce cadre. Ceci est d'autant plus préoccupant que l'on constate que la lutte contre le terrorisme est un prétexte abusivement mis en avant.

Peut-on vraiment mettre dans un même système une personne qui aurait commis un délit « mineur », une personne qui aurait commis des crimes sexuels et une personne qui aurait commis un acte terroriste ? Sous cette forme, il y a automatiquement un conflit entre le principe de proportionnalité et celui de finalité.

5.2. Finalités d'ECRIS : garder la trace des condamnations dans l'Union européenne des citoyens de l'UE

ECRIS permet aux États de l'UE de garder, au sein du pays de nationalité d'une personne condamnée, l'historique des condamnations prononcées dans d'autres États membres et ce à des fins multiples.

5.2.1. Maintenir les casiers judiciaires des citoyens de l'UE à jour et complet

En tant que système informatisé, ECRIS a pour but de faciliter la transmission d'informations issues du casier judiciaire d'un citoyen européen entre des États membres concernés. Le système concerne spécifiquement des informations sur les condamnations pénales prononcées par des cours pénales et, si possible, d'autres informations telles que les circonstances particulières qui ont motivé la décision. En conséquence, l'État membre qui a imposé une peine à un ressortissant d'un autre État membre utilisera ECRIS pour informer l'État de nationalité de la personne, de cette nouvelle condamnation. Ensuite, l'État membre de nationalité ajoutera cette condamnation au casier judiciaire de la personne. Le but étant que chaque État membre tienne les casiers judiciaires de leurs ressortissants à jour et complets, même avec des condamnations qui ont été prononcées dans un autre État. Sur ce dernier point, on peut se demander comment, dans la pratique, un État intègre une condamnation pour une infraction qui n'existe pas dans sa législation ?

46. C'est le cas lorsque l'on prend l'exemple de deux femmes qui ont vécu exactement la même situation : grossesse non désirée puis avortement au bout de la même durée de grossesse. L'une voit son avortement inscrit sur son casier judiciaire dans un État (car avortement illégal), l'autre non. Ces deux femmes postulent ensuite à un même emploi dans la fonction publique, dans un même pays, et ont les mêmes compétences. Dans l'hypothèse où l'administration peut consulter le casier judiciaire « complet » des deux femmes, elle aura alors connaissance de l'avortement de l'une, et non de celui de l'autre. Or, derrière chaque administration, il y a une personne, qui raisonne avec sa propre conscience : aussi, même si la législation de l'État ne permet pas de discriminer à l'embauche sur la base d'un avortement passé, il faut garder à l'esprit que plus on divulgue des données personnelles, lesquelles ne sont pas forcément utiles en considération du but poursuivi, plus on a de risques d'être discriminé.
47. Déclaration sur la lutte contre le terrorisme, Bruxelles, le 25 mars 2004

5.2.2. Informer des autorités judiciaires sur les condamnations passées d'une personne à juger

Les États membres doivent aussi transmettre des informations sur les condamnations (décidées en national au sein de l'UE) de leurs ressortissants aux autorités centrales des autres États membres, lorsqu'elles le demandent, et ce dans le cadre de procédures pénales. Cela est souvent le cas lorsqu'une autorité judiciaire doit rendre un jugement à l'encontre d'un ressortissant d'un autre pays de l'UE et souhaite connaître, entre autre, si la personne a des antécédents criminels. Toutefois, comme il a été dit plus tôt, il semble que toutes les condamnations soient envoyées et ne sont pas triées en fonction des besoins du demandeur, ce qui rend la finalité d'ECRIS dangereuse.

5.2.3. Savoir qu'une personne a été déchue de ses droits

ECRIS sert également à informer les acteurs appropriés si un citoyen a perdu certains de ses droits en raison d'une condamnation. Cette information est disponible même sans aucune procédure judiciaire. C'est le cas lorsque la législation d'un pays autorise ou oblige un employeur à s'informer sur les éventuelles condamnations d'un candidat, ce qui.est le cas dans le cadre de certains emplois (ex : au contact d'enfants, dans la sécurité…) mais aussi lorsqu'une autorité doit connaître l'antécédent d'une personne avant de la laisser exercer certaines professions (ex : médecins, avocats…). Selon les pays, l'information peut ressembler à un certificat de « bonne conduite » ne contenant aucune condamnation ou un extrait de casier judiciaire. Il est à craindre si cette approche n'est pas très bien régulée (entre autre par la création d'une liste d'emplois visés légalement établie), et sans erreurs que cela nuise à la réinsertion d'un individu, après une peine pourtant exécutée, et à son intégration dans un pays tout en ayant des conséquences sur son droit de choisir librement un emploi.

5.2.4. Possibilités futures

Actuellement, ECRIS ne concerne que les citoyens de l'Union européenne mais à terme l'UE souhaite intégrer toutes les personnes résidant sur son territoire. Les États membres étudient l'idée de compléter ECRIS avec un « Index européen des ressortissants de pays tiers ayant fait l'objet de condamnation dans l'UE », qui porterait donc sur les résidants étrangers d'un État membre, en vue d'échanger à leurs sujets des informations sur leurs condamnations pénales antérieures[48].

5.3. Un régime juridique critiquable

5.3.1. Les textes d'ECRIS : une porte ouverte à l'interprétation

ECRIS a été créé par la Décision Cadre du Conseil 2009/315/JAI du 26 février 2009 et mis en œuvre par la décision du Conseil 2009/316/JAI du 6 Avril 2009. Dans chaque État membre, les lois et règlements nationaux en lien avec les casiers judiciaires, ainsi que ceux mettant en œuvre la législation européenne et internationale sont également applicables à ECRIS.

Les textes de mise en œuvre d'ECRIS sont fortement critiquables. Tout d'abord, ils manquent de clarté voire contiennent des lacunes, laissant beaucoup trop de place à l'interprétation. Par exemple, il n'est pas mentionné la façon dont un État va transposer une condamnation qui n'existe pas dans sa législation. En outre, fréquemment les textes renvoient aux régimes nationaux. On constate ainsi dans le manuel de procédure de 2010[49], que dans certains États il n'y a pas obligation de demander à une personne son consentement lors d'envois d'informations à une autorité administrative en dehors de procédures criminelles, ou encore la personne elle-même doit donner une raison lorsqu'elle souhaite faire

48. Pour plus d'informations, voir : http://www.publications.parliament.uk/pa/cm201213/cmselect/cmeuleg/86-xviii/8619.htm, http://ec.europa.eu/justice/criminal/european-e-justice/ecris/

une demande d'extrait de casier judiciaire. On note aussi que pour des questions d'identification, certains États demandent des informations personnelles supplémentaires (ex : le nom des parents, les empreintes), que l'État demandeur d'informations devra fournir si elle les possède, lors de ses demandes.

En outre, plusieurs principes de base de la protection des données sont mis à mal par l'absence de qualité des textes. En effet, comme abordé plus haut, la finalité est trop large et ce particulièrement par l'intégration de la politique anti-terroriste. La proportionnalité manque de précision, ne serait-ce que sur les informations qu'il faut envoyer à une autorité judiciaire sur un citoyen, et ne semble pas avoir été suffisamment délimitée pour la mise en œuvre pratique. La limitation dépendant de chacun des systèmes nationaux, le traitement inéquitable des citoyens qui en résulte est critiquable. Dans son Avis du 16 Septembre 2008, le CEPD recommande que seule la personne concernée puisse faire une demande d'informations de son casier judiciaire. Il souligne aussi qu'il n'a pas été suffisamment défini dans quelles circonstances autres que celles relatives à une procédure criminelle des demandes d'informations sur les casiers judiciaires peuvent être introduites. Il est à regretter que la majeure partie des éléments clés proposés par le CEPD n'ait pas été intégrée au texte final d'ECRIS.

De plus, les informations échangées sont traduites automatiquement par le biais de deux tables de référence codées (délits et peines). Ces tables n'uniformisent pas les différents systèmes nationaux que ce soit sur les définitions des délits ou les durées des peines. Il s'agit là uniquement d'amener une compréhension des systèmes nationaux.

La fiabilité de cette méthode peut être mise en question. Au-delà d'accroître les possibilités d'erreurs lors de l'encodage des informations, ne pas connaître au préalable la législation nationale du pays de provenance, laisse une trop grande place à l'interprétation des délits ce qui est fortement nuisible aux personnes.

Enfin, le flou sur le contrôle du traitement amène à se demander si les principes de sécurité, de droits des personnes et de transparence sont bien respectés.

5.3.2. Une protection des données faibles, des garanties manquantes et la nécessite d'un texte fort

Au niveau européen, les législations sur la protection des données qui s'appliquent à ECRIS sont la Convention Européenne des Droits de l'Homme, la Convention 108 du Conseil de l'Europe de 1981 et la Décision Cadre du Conseil 2008/977/JAI du 27 Novembre 2008, fortement critiquée car ne protégeant pas suffisamment les individus. Ce dernier a été intégré suite à l'Avis du CEPD de 2008 qui demandait d'attendre l'adoption de la Décision Cadre avant d'adopter ECRIS, pour qu'il y ait un cadre minimum de protection.

Il est important de noter que, à la différence des autres systèmes étudiés dans cette monographie, la Directive 95/46/CE (Directive 1995) ne s'applique pas à ECRIS. En effet, elle ne s'applique pas dans les domaines de la coopération judiciaire et policière en matière pénale. Néanmoins, la réforme de la Directive 1995 propose une Directive sur la protection des données personnelles traitées dans le cadre de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, qui supprimerait le cadre actuel de la Décision 2008/977/JAI.

Le Règlement (CE) n°45/2001, qui porte sur la responsabilité des Institutions européennes, ne s'applique pas à ECRIS non plus. Par conséquent, aucune Institution de l'UE n'est responsable d'ECRIS. Ainsi, le Contrôleur européen à la Protection des données (CEPD) n'est pas compétent pour superviser le traitement des données et il n'y a aucune coordination entre le CEPD et les Autorités nationales de protection des données dans la mise en œuvre et le contrôle du système. Il est à souligner que dans son Avis de 2008, le CEPD en avait fait la demande, en vain. Ceci est dangereux pour les citoyens euro-

49. Note from Council Secretariat to Delegations, Council Decision on the exchange of information extracted from criminal records – Manual of Procedure, 21 April 2010

péens. En effet, il n'y a aucun contrôle des échanges faits entre États membres au niveau supranational ce qui laisse une marge d'erreurs possibles assez grande et affaiblit de façon générale la protection des citoyens. En outre, ne pas mettre à jour les informations du casier judiciaire d'un individu peut avoir de graves conséquences sur la personne. Aussi un contrôle rigoureux de ces échanges est-il plus que primordial.

Cette crainte sur le contrôle est accrue avec le flou autour des entités en charge de contrôler le traitement des données au niveau national. Dans la mesure où la Directive 1995 ne s'applique pas, ce sont les lois nationales qui s'appliquent mais certaines des Autorités Nationales de Protection des Données peuvent ne pas être compétentes pour le contrôle de ces fichiers. Dans le cadre des pays étudiés pour ce projet, c'est le cas par exemple du Luxembourg où le contrôle des fichiers de police et de justice incombe à une autorité de contrôle spécifique distincte de l'Autorité de Protection des Données et qui est présidée par le Procureur d'État.

En outre, les mesures de sécurité énoncées dans le texte d'ECRIS, stipulent qu'aucune autorité d'un État membre ne peut accéder aux bases de données d'un autre État membre que le sien, et que les États membres doivent assurer la confidentialité et l'intégrité des informations des casiers judiciaires transmises à d'autres États membres. Toutefois, ces mesures de sécurité ne sont pertinentes que s'il y a un réel contrôle sur la mise en œuvre d'ECRIS.

Entre une décision-cadre faible, des textes obsolètes et des textes clés absents, on peut constater que la protection des personnes concernées par ECRIS est assez faible. Aussi, est-il nécessaire, que le projet de directive cité plus haut sur la coopération policière et judiciaire, aboutisse et soit suffisamment fort pour empêcher ce type de dérives et assurer une vraie protection des personnes concernées.

Dans son état actuel, la législation d'ECRIS n'offre pas les garanties minimum de protection des personnes.

5.3.3. Législations nationales : multiplicité de systèmes et la possibilité de demander un casier judiciaire à des fins professionnelles

Les lois et régulations nationales relatives à la structure des systèmes nationaux des casiers judiciaires, celles relatives à la définition des infractions et au cas où leurs informations peuvent être utilisées, s'appliquent aux informations échangées au travers d'ECRIS.

La Convention du Conseil de l'Europe sur l'assistance mutuelle en matière criminelle de 1959 est également pertinente pour ECRIS. Des dispositions spécifiques dans d'autres textes européens font référence aussi à l'utilisation d'ECRIS:

- L'article 10 de la Directive 2011/93/UE autorise les employeurs à être informés des condamnations antérieures des candidats en rapport avec les délits commis vis-à-vis des enfants et des éventuelles disqualifications pour exercer des activités impliquant des contacts avec les enfants. Le consentement du candidat est requis.

- L'article 50 de la Directive 2005/36/CE sur la reconnaissance des qualifications professionnelles, autorise les autorités nationales compétentes à requérir le casier judiciaire -de moins de 3 mois- d'un professionnel souhaitant s'établir dans leur État Membre. C'est le cas des professions dîtes « réglementées » et dont les métiers précisément diffèrent d'un pays à l'autre. Parmi ces professions se trouvent les professionnels de la santé (ex : médecins, infirmières…), de la sécurité (ex : vigile, pompier), du droit (ex : avocat, notaire), les métiers aéroportuaires ou encore les architectes[50].

Comme il n'existe aucune harmonisation au niveau européen des systèmes de casiers judiciaires et de leur utilisation, la mise en œuvre d'ECRIS inclut une multitude de textes nationaux et donc plusieurs procédures nationales ce qui accroît les risques de détournement et complique le suivi d'ECRIS.

5.4. Les données collectées et la durée de stockage

Pour toute condamnation qui apparaît dans un casier judiciaire, l'État qui a condamné une personne transmettra à (aux) État(s) de nationalité de la personne les informations suivantes :

50. Pour plus d'informations, voir la base de données de la Commission européenne sur les professions réglementées : http://ec.europa.eu/internal_market/qualifications/regprof/index.cfm?fuseaction=regProf.index&lang=en

Informations obligatoires	**Informations facultatives**	**Informations complémentaires**	**Informations secondaires**
▪ **Sur la personne condamnée :** nom, prénom, date de naissance, lieu de naissance (ville et pays), le sexe, la nationalité et - le cas échéant - nom (s) précédent	*Renseignements qui doivent être transmis si l'État de condamnation les insère habituellement dans les casiers judiciaires*	*Renseignements qui doivent être transmis si l'État de condamnation les insère habituellement dans les casiers judiciaires*	*Renseignements possibles d'être envoyées*
▪ **Sur la nature de la condamnation :** date de condamnation, nom de la cour, date à laquelle la décision est devenue définitive	▪ les noms des parents de la personne condamnée; ▪ ▪ le numéro de référence de la déclaration de culpabilité;	▪ le numéro d'identité de la personne condamnée, ou le type et le numéro du document d'identification de la personne; ▪	Informations sur des circonstances atténuantes ou aggravantes liées délit[4]
▪ **Sur l'infraction ayant donné lieu à la condamnation :** date de l'infraction ayant amené la condamnation et le nom ou la qualification juridique de l'infraction ainsi que la référence aux dispositions légales applicables	▪ ▪ le lieu de l'infraction; ▪	▪ empreintes digitales, qui ont été prises de cette personne ▪	
▪ **Sur le contenu de la condamnation :** notamment la peine ainsi que les peines complémentaires éventuelles, les mesures de sécurité et les décisions ultérieures modifiant l'exécution de la peine	▪ Les droits perdus résultant de la condamnation;	▪ le cas échéant, le pseudonyme et / ou alias.	

Cependant, ces différenciations entre les données n'apparaissent pas dans le formulaire de demandes d'informations d'extraits de casiers judiciaires[51]. En effet, les différentes catégories d'information ne sont pas visibles. En outre, pour les données d'identification de la personne, la mention en astérisque *« Pour faciliter l'identification de la personne, il convient de fournir autant de renseignements que possible »,* porte à confusion sur ce qui est légalement possible d'inclure dans le formulaire.

En ce qui concerne **la durée de stockage** des condamnations dans les casiers judiciaires, la législation n'est pas claire. Cependant, comme le cadre d'une condamnation dépend de chaque État membre, on peut présumer que la durée dépendra du pays qui est à l'origine de la condamnation.

En prenant l'exemple d'un ressortissant français qui a commis un crime en Royaume-Uni : lorsque le Royaume-Uni enverra les informations sur la condamnation à la France, la France appliquera les règles du Royaume-Uni sur la période de conservation. Ainsi, si cette condamnation est conservée 10 ans au Royaume-Uni alors qu'elle n'est conservée que 2 ans en France, la condamnation doit rester 10 ans sur le casier judiciaire du citoyen français. Le Royaume-Uni devra alors informer la France lorsque cette dernière devra retirer la condamnation à la fin des 10 ans.

Cet élément complexifie encore ECRIS et entraîne un traitement différent entre chaque citoyen de l'UE pour un même délit.

5.5. La mise en œuvre opérationnelle

ECRIS n'est pas un système centralisé mais bien un système décentralisé. En comparaison des autres systèmes étudiés, ECRIS ne possède pas de base de données centrale. Tous les casiers judiciaires sont tenus au niveau national. Donc ECRIS se base sur l'échange direct d'information entre les autorités nationales compétentes. On peut décrire ECRIS comme étant une méthode permettant aux États membres de savoir ce qui se trouve dans les casiers judiciaires de leurs nationaux ou d'autres ressortissants de l'UE qu'ils poursuivent en justice.

Chaque État membre doit désigner une ou plusieurs autorités en charge de gérer les demandes en rapport avec la base de données des casiers judiciaires. Elles sont appelées « autorités compétentes » ou « autorités centrales ». Elles sont les seules à pouvoir accéder aux casiers judiciaires de leurs citoyens.

Leurs tâches consistent donc à :
- Transmettre à l'État de nationalité d'une personne reconnue coupable sur leur territoire les informations sur les condamnations. Cela inclut également l'envoi de toute modification apportée à la condamnation (nouvelle entrée, suppression, modification).
- Recevoir et conserver les informations sur leurs ressortissants transmisses par un autre État, qui comprend également la mise à jour des casiers judiciaires selon les modifications apportées par cet État.
- Transmettre des informations sur les condamnations de leurs ressortissants à la demande d'une autorité centrale d'un autre État lors de procédures pénales engagées à l'encontre de leurs ressortissants mais (aussi de procédures non pénales dans le cadre d'un extrait de casier judiciaire ou certificat de bonne conduite. L'information doit être mise à jour.

Ces acteurs peuvent être :
- Le ministère de la justice (exemple en Italie) ou un département particulier du ministère de la Justice (exemple au Luxembourg)
- Un service administratif précis en charge des casiers judiciaires (exemple en France)
- La police nationale ou un de ses départements (exemple au Danemark)
- Le ministère de l'Intérieur (exemple en Lituanie)

51. Annexe Décision Cadre 2009/315/JAI

En ce qui concerne le Royaume-Uni, et en raison du système décentralisé, il existe une autorité de coordination et des autorités régionales. Ces trois juridictions que sont l'Ecosse, l'Irlande du Nord et réunit ensemble, le Pays de Galles et l'Angleterre, ont des systèmes historiques pénaux séparés, des infractions différentes et des sanctions qui diffèrent[52]. L'autorité de coordination envoie donc les demandes faites par les États membres à l'autorité régionale responsable. L'autorité de coordination est également en charge de transmettre les réponses aux États ayant fait une demande.

5.6. Les droits d'information et de rectification des citoyens

Le droit pour un individu d'accéder aux informations conservées dans son casier judiciaire dépend de la législation nationale de son État membre de nationalité. Toutefois, en vertu du droit à la protection des données personnelles existant dans les pays étudiés pour ce projet, il y a un droit de connaître les fichiers existants et les données personnelles qui y sont contenues.

On constate qu'en Allemagne et en France, pour éviter toute pression externe, une personne peut consulter l'intégralité de son casier judiciaire mais aucune copie ne lui sera délivrée. Ceci ne s'applique pas à la République tchèque et au Portugal. En outre, certains garantissent un accès sans réserve, alors que d'autres désirent connaître la raison de la demande d'accès.

Pour la rectification, cela dépend aussi du droit national. Cependant, comme les informations doivent toujours être mises à jour avant d'être transmises, on peut présumer que les pays qui donnent à la personne concernée un accès à son casier judiciaire permettent aussi la rectification d'information dans ce casier ou fournissent la possibilité d'un recours judiciaire. Dans tous les cas, les institutions en charge se trouvent au niveau national.

52. Note from Council Secretariat to Delegations, Council Decision on the exchange of information extracted from criminal records – Manual of Procedure, p 103, 21 April 2010

(Footnotes)

1 Pour les ressortissants d'un pays tiers ou apatrides, interpellé lors du franchissement irrégulier d'une frontière extérieure, on parle là d'un individu qui : n'a pas fait l'objet d'une décision de refoulement ; a fait l'objet d'une décision de refoulement mais est toujours présent physiquement sur le territoire des États membres et ne fait pas l'objet d'une mesure de détention avant son éloignement qui est basé sur la décision de refoulement.

2 En cas de transfert (Règlement 603/2013, Article 10, paragraphe b) cette date est celle du transfert.

3 En cas de transfert (Règlement 603/2013, Article 10, paragraphe b) cette date est celle du transfert.

4 Art. 11 (1) c of Framework Decision 2009/315/JHA says that the transmission of these supplementary information are not compulsory.

LDH, Ligue des droits de l'Homme
www.ldh-france.org

AEDH, Association européenne
pour la défense des droits de l'Homme
www.aedh.eu

Humanistische Union
www.humanistische-union.de

HCLU, Hungarian Civil Liberties Union
www.tasz.hu/en

ALOS-LDH, Action Luxembourg Ouvert
et Solidaire - Ligue des droits de l'Homme
www.ldh.lu

MEDEL, Magistrats européens
pour la démocratie et les libertés
www.medelnet.eu

Cette publication a été éditée avec le soutien financier du programme Fundamental Rights de la Commission européenne.