MANUEL

Guide pour la prévention du profilage illicite aujourd'hui et demain

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

De nombreuses informations sur l'Agence des droits fondamentaux de l'Union européenne (FRA) sont disponibles sur l'internet. Elles peuvent être consultées sur le site web de la FRA à l'adresse fra.europa.eu.

Europe Direct est un service destiné à vous aider à trouver des réponses aux questions que vous vous posez sur l'Union européenne.

Un numéro unique gratuit (*):

00 800 6 7 8 9 10 11

(*) Les informations sont fournies à titre gracieux et les appels sont généralement gratuits (sauf certains opérateurs, hôtels ou cabines téléphoniques).

Photos (couverture & à l'intérieur, de gauche à droite): © stock.adobe.com-Savvapanf Photo.

D'autres informations sur l'Union européenne sont disponibles sur l'internet (http://europa.eu).

Luxembourg Office des publications de l'Union européenne, 2019

Print: ISBN 978-92-9474-250-6 doi:10.2811/34208 TK-06-18-031-FR-C
PDF: ISBN 978-92-9474-246-9 doi:10.2811/65391 TK-06-18-031-FR-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Guide pour la prévention du profilage illicite aujourd'hui et demain

Table des matières

Figures et tableaux

Acronymes et abréviations

AIPD	Analyse d'impact relative à la protection des données
CDH	Comité des droits de l'homme des Nations unies
CEDH	Convention européenne des droits de l'homme
CEPD	Contrôleur européen de la protection des données
CJUE	Cour de justice de l'Union européenne
CouEDH	Cour européenne des droits de l'homme
EES	Système d'entrée/sortie
ENISA	Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information
ETIAS	Système européen d'information et d'autorisation concernant les voyages
EU-MIDIS	Enquête de l'Union européenne sur les minorités et la discrimination
FRA	Agence des droits fondamentaux de l'Union européenne
Frontex	Agence européenne de garde-frontières et de garde-côtes
GT art.29	Groupe de travail article 29 sur la protection des données
HCDH	Haut-Commissariat des Nations unies aux droits de l'homme
NU	Nations unies
OSCE	Organisation pour la sécurité et la coopération en Europe
RGPD	Règlement général sur la protection des données
SIS II	Système d'information Schengen
UE	Union européenne
VIS	Système d'information sur les visas

Introduction

Les évolutions technologiques ont entraîné un recours accru au profilage dans un large éventail de contextes, dont la commercialisation, l'emploi, la santé, la finance, l'application de la loi, le contrôle aux frontières et la sécurité. Ces dernières années, les États membres de l'Union européenne (UE) ont accordé une plus grande attention à l'utilisation des outils de profilage par les agents de police et les fonctionnaires chargés de la gestion des frontières. Le profilage est communément et légitimement utilisé par les agents de police et les gardes-frontières afin de prévenir les infractions pénales, d'enquêter sur celles-ci et de poursuivre leurs auteurs, ainsi que de prévenir et de détecter l'immigration irrégulière. Toutefois, un profilage illicite peut saper la confiance dans les autorités, en particulier envers la police, et stigmatiser certaines communautés. La perception d'une utilisation discriminatoire du profilage peut ainsi cristalliser les tensions entre les communautés et les autorités chargées de faire appliquer la loi.

Le présent guide explique ce qu'est le profilage, les cadres juridiques qui le régissent, et les raisons pour lesquelles le profilage légal n'est pas seulement nécessaire pour respecter les droits fondamentaux : il est crucial pour l'efficacité des activités de la police et de la gestion des frontières. Le guide fournit également des orientations pratiques sur la manière d'éviter tout profilage illicite dans les opérations de police et de gestion des frontières. Les principes et les pratiques énoncés dans le guide sont étayés par des exemples, des études de cas et la jurisprudence dans l'ensemble de l'UE et au-delà.

Pourquoi avons-nous besoin de ce guide ?

Le profilage soulève un certain nombre de problèmes liés aux droits fondamentaux [1]. Les risques que certaines de ces pratiques enfreignent des principes juridiques bien établis, tels que l'égalité et la non-discrimination, ou les droits au respect de la vie privée et à la protection des données, existent. En outre, des interrogations subsistent concernant l'efficacité de ces pratiques afin de lutter contre les activités illégales, ainsi que les éventuelles conséquences négatives pour les relations entre les autorités (y compris la police et la gestion des frontières) et les communautés qu'elles desservent.

En réponse à ces préoccupations, l'Agence des droits fondamentaux de l'Union européenne (FRA) a publié, en 2010, un guide intitulé *Pour des pratiques de police plus efficaces — Guide pour comprendre et prévenir le profilage ethnique discriminatoire*. Axé sur l'utilisation du profilage par la police, le guide se penchait plus particulièrement sur l'exercice des pouvoirs de contrôle et de fouille. Le guide entendait doter les agents d'outils permettant d'éviter la mise en place de techniques de profilage discriminatoire fondées sur l'appartenance ethnique.

Depuis lors, les avancées technologiques ont considérablement modifié la nature du profilage. Une grande partie de celui-ci est désormais fondée sur les résultats d'analyses algorithmiques basées sur de larges banques de données. Sur le plan juridique, les nouvelles règles en matière de protection des données applicables dans l'ensemble de l'UE à partir de mai 2018 établissent de nouvelles normes pour la collecte, l'analyse et l'utilisation de données à caractère personnel.

Le présent guide intègre ces changements et, tout en s'appuyant sur sa version antérieure de 2010, il en élargit la portée pour s'adapter aux nouvelles réalités juridiques et pratiques. Il adopte une approche plus globale du profilage illicite en intégrant :

- le profilage dans le contexte de la gestion des frontières ;
- le profilage discriminatoire sur la base de tous les motifs, y compris la nationalité, l'âge ou le sexe, en plus de l'origine ethnique ;
- le profilage algorithmique.

1 Voir FRA (2018e), p. 85-87 ; FRA (2017c), p. 88-89 ; et FRA (2016), p. 83-85.

Cette version de 2019 contient également de nouveaux exemples et des études de cas reflétant les évolutions et les innovations en matière de profilage.

À qui s'adresse ce guide ?

Le présent guide s'adresse en premier lieu aux formateurs des agents de police et des fonctionnaires chargés de la gestion des frontières. Il peut également apporter un soutien aux agents occupant des postes de niveau intermédiaire afin de les aider à mettre en œuvre des techniques de profilage de manière licite. Il vise à mieux faire comprendre la théorie et la pratique du profilage, et à illustrer concrètement la manière dont le profilage peut être mené dans le respect des droits fondamentaux.

Le guide couvre le profilage par les agents de police de première ligne — par exemple lors des opérations de contrôle et de fouille — et les vérifications effectuées par les gardes-frontières aux points de passage frontaliers, notamment lorsqu'une décision est prise de renvoyer une personne pour une vérification plus approfondie de « deuxième ligne ». Dans le domaine de la gestion des frontières, il s'agit d'une aide à la formation destinée aux personnes qui dispensent les programmes de base communs pour la formation des gardes-frontières conformément à l'article 36, paragraphe 5, du règlement relatif au corps européen de garde-frontières et de garde-côtes [règlement (UE) 2016/1624].

Le guide traite également du profilage fondé sur l'analyse de grands ensembles de données, y compris celles régies par le droit de l'Union européenne. Le profilage dans d'autres circonstances, comme le profilage mené dans le secteur privé à des fins commerciales, dépasse le cadre du présent guide. La FRA mène des recherches supplémentaires sur ce sujet [2].

Comment utiliser ce guide

Ce guide donne un aperçu des grands principes et pratiques du profilage dans le contexte de l'application de la loi et de la gestion des frontières. Il peut être lu dans son intégralité ou utilisé comme référence pour soutenir des activités de formation.

Le guide contient trois chapitres. Le premier chapitre définit la notion de profilage, précisant les circonstances dans lesquelles celui-ci est illicite, et décrit les éventuelles conséquences négatives que celui-ci peut avoir, non seulement sur les individus et les

2 Voir le projet de la FRA sur L'intelligence artificielle, les mégadonnées et les droits fondamentaux.

communautés, mais également sur l'exercice des pouvoirs de police et de gestion des frontières. Le deuxième chapitre détaille les principes et pratiques qui devraient guider les agents de police et les gardes-frontières afin que ceux-ci mettent en œuvre des activités de profilage légales. Enfin, le troisième chapitre se concentre sur le profilage algorithmique. Étant donné que la pratique en la matière n'est pas très développée, cette section contient moins d'exemples concrets. Au lieu de cela, elle présente les principaux risques posés aux droits fondamentaux par l'établissement de profils informatisés et expose les principales exigences juridiques établies par le règlement général sur la protection des données (RGPD) et la directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale (directive « police »).

Plusieurs élément schématiques illustrent les différents principes du guide. Les points clés résument les principaux messages et sont mis en évidence dans des encadrés jaunes. Les encadrés bleu mettent l'accent sur des aspects essentiels du cadre juridique, et les encadrés verts illustrent les principes par des exemples concrets. Les autres encadrés soulignent des points importants sur lesquels il y a lieu de se concentrer, des études de cas et des exemples de la jurisprudence. Malgré les efforts consentis pour diversifier les études de cas, un nombre disproportionné d'exemples proviennent du Royaume-Uni. En effet, le Royaume-Uni s'est attaqué au profilage illicite dès les années 1980, alors que d'autres États membres n'ont reconnu la pratique du profilage illicite que très récemment. Cela signifie que le Royaume-Uni dispose de politiques et de pratiques plus étoffées et plus mûres en la matière, dont on peut s'inspirer.

Comment le guide a-t-il été élaboré ?

La FRA a organisé une réunion avec des experts de différents domaines afin d'examiner un avant-projet de guide et de l'assister dans la production du produit final.

À cet égard, la FRA tient à adresser ses remerciements aux experts du Haut-Commissariat des Nations unies aux droits de l'homme (HCDH), à l'Agence européenne de garde-frontières et de garde-côtes (Frontex), au Bureau des institutions démocratiques et des droits de l'homme (BIDDH) de l'Organisation pour la sécurité et la coopération en Europe (OSCE), à Amnesty International, au Réseau européen contre le racisme (ENAR), au Centre international pour le développement des politiques migratoires (CIDPM), au FIZ Karlsruhe, Leibniz Institut für Informationsinfrastruktur GmbH, au European Digital Rights (EDRi), à l'Open Society Initiative for Europe et aux représentants du Défenseur des droits français, des forces de police néerlandaises, danoises et autrichiennes et aux gardes-frontières polonais pour leur précieux retour d'information lors de l'élaboration du guide.

Résumé des principaux points

1. Les caractéristiques protégées ne peuvent jamais être la seule base du profilage

- Le profilage consiste à **catégoriser les individus** en fonction de leurs caractéristiques.
- Pour recueillir et traiter les **données à caractère personnel**, les autorités policières et les autorités chargées de la gestion des frontières doivent veiller à ce que la collecte et le traitement des données aient une base juridique, un objectif valide et légitime, et soient nécessaires et proportionnés.
- **Les caractéristiques protégées** telles que la race, l'origine ethnique, le sexe ou la religion peuvent figurer parmi les facteurs pris en compte par les autorités policières et les gardes-frontières pour exercer leurs pouvoirs, mais elles **ne peuvent être la seule ou principale raison de distinguer un individu.** Pour de plus amples informations sur les « caractéristiques protégées », voir section 1.2.1.
- Le profilage qui repose uniquement ou principalement sur une ou plusieurs caractéristiques protégées équivaut à une discrimination directe et, par conséquent, **enfreint les droits et libertés de la personne** et est **illégal**.

2. Tout contact avec les personnes doit être respectueux, professionnel et informatif

- Un **contact de bonne qualité** ne permet pas, en soi, d'éliminer le profilage fondé sur des partis pris mais est plus susceptible de rendre le contact plus efficace et de réduire l'incidence négative éventuelle du contrôle réalisé par un agent de police ou un garde-frontière. Dans le domaine de la gestion des frontières, un comportement professionnel et respectueux constitue spécifiquement une obligation juridique.
- **Un comportement professionnel et respectueux** augmente généralement la satisfaction d'une personne vis-à-vis du contact.
- **Expliquer les raisons du contrôle** d'une personne contribue à renforcer la confiance du public dans les opérations de police et de gestion des frontières, et réduit la perception d'un profilage fondé sur des partis pris.
- Le respect et la politesse, toutefois, **ne justifient jamais des vérifications aux frontières ou des contrôles et des fouilles illégaux**.

3. Le profilage doit être fondé sur des motifs objectifs et raisonnables

- Pour être licites, les contrôles et les renvois aux vérifications aux frontières de deuxième ligne doivent **être basés sur des motifs raisonnables et objectifs** de suspicion.
- Les caractéristiques personnelles peuvent être utilisées comme facteurs légitimes de profilage. Toutefois, pour éviter toute discrimination, **il doit *également* exister des motifs raisonnables de suspicion** fondés sur des informations autres que les caractéristiques protégées.
- Les actions des agences répressives et de gestion des frontières fondées sur des **renseignements spécifiques et actualisés** sont plus susceptibles d'être **objectives**.
- Il importe que la décision de contrôler une personne ou de la soumettre à une vérification aux frontières de deuxième ligne ne se **fonde pas uniquement sur une *impression*** d'un officier à son sujet, étant donné que cela risque d'être fondé sur des partis pris, des stéréotypes et/ou des préjugés.

4. Le profilage illicite a une incidence négative sur les activités de la police et la gestion des frontières

- **Le profilage illicite sape la confiance dans la police et les gardes-frontières.** Il peut entraîner une détérioration de la relation entre la police/les gardes-frontières et les membres de minorités et d'autres communautés qui peuvent se sentir exclus. Ce sentiment d'injustice peut ébranler la confiance de certains individus et groupes dans la police et d'autres autorités, les incitant éventuellement à moins déclarer les crimes à la police et à se montrer moins coopératifs avec les autorités. Les autorités peuvent, à leur tour, nourrir une certaine méfiance à l'égard de certains groupes, ce qui peut entraîner davantage de pratiques de profilage illicite.
- **Le profilage illicite nuit à l'efficacité du profilage**, étant donné que la fréquence des contrôles des individus, que ce soit par la police ou à la frontière, ne correspond pas nécessairement à la fréquence des infractions commises au sein des différents groupes.
- Il existe un risque de **prophétie autoréalisatrice** lorsqu'un groupe minoritaire est ciblé de manière disproportionnée par les agents de police ou de gestion des frontières, ce qui se traduit par une augmentation du nombre d'arrestations ou de vérifications à la frontière.

5. Le profilage illicite a des conséquences juridiques et financières et les agents sont tenus de rendre des comptes

- Les agents de police et de la gestion des frontières sont **responsables** d'assurer un profilage respectueux des lois.
- **La collecte de données fiables, exactes et actuelles** est essentielle pour garantir la responsabilité.
- **Des mécanismes de plainte efficaces** peuvent à la fois décourager les abus de pouvoir et contribuer à rétablir la confiance du public dans les opérations de la police et des autorités chargées de la gestion des frontières.
- **Des réunions de retour d'information avec les citoyens** (afin d'écouter leurs avis, de discuter du profilage et de recueillir un retour d'information sur les opérations) permettent de tirer des enseignements importants et d'améliorer les actions de profilage.

6. Le profilage algorithmique doit respecter des garanties spécifiques en matière de protection des données

- Lors de l'élaboration et de l'utilisation du profilage algorithmique, des **partis pris** peuvent être introduits à chaque étape du processus. Pour éviter cette situation et les éventuelles violations ultérieures des droits fondamentaux, les **experts en technologies de l'information et les agents chargés de l'interprétation des données doivent avoir une vision claire des droits fondamentaux**.
- L'utilisation de **données fiables** est essentielle. La saisie de données reflétant des partis pris existants ou provenant de sources non fiables dans un algorithme produiront des résultats biaisés et peu fiables.
- Le profilage algorithmique doit être **légitime, nécessaire et proportionné**.
- Le traitement des données doit avoir une **finalité spécifique**.
- Les individus ont le **droit d'être informés**, en recevant des informations sur les données à caractère personnel qui sont collectées et stockées, sur le traitement et sur leur finalité, ainsi que sur leurs droits.
- Les données doivent être **collectées, traitées et stockées en toute sécurité**. Les autorités doivent conserver une trace des activités de traitement (y compris de ce qui est fait aux données) et des registres les concernant (y compris les informations sur la ou les personnes ayant accès aux données).
- Le traitement illicite de données doit être **évité et détecté** : 1) par des analyses d'impact préalables, et 2) par l'utilisation d'outils de protection de la vie privée intégrés dans l'algorithme « dès la conception ».

Sites web utiles

Union européenne
Cour de justice de l'Union européenne (CJUE) : http://www.curia.eu
Législation de l'UE : http://eur-lex.europa.eu/
Agence des droits fondamentaux de l'Union européenne (FRA) : http://www.fra.europa.eu/fr
Parlement européen : http://www.europarl.europa.eu/portal/fr

Conseil de l'Europe
Comité des ministres du Conseil de l'Europe : http://www.coe.int/fr/web/cm
Cour européenne des droits de l'homme (CouEDH) : http://www.echr.coe.int

Nations unies
Haut-Commissariat des Nations unies aux droits de l'homme (HCDH) : http://www.ohchr.org

Lutte contre la discrimination
Commission européenne contre le racisme et l'intolérance (ECRI) : http://www.coe.int/ecri
Réseau européen des organismes de promotion de l'égalité (Equinet) : http://www.equineteurope.org/
Organismes nationaux de promotion de l'égalité : http://www.equineteurope.org/-Equinet-Members-

Protection des données
Contrôleur européen de la protection des données (CEPD) : https://edps.europa.eu/
Comité européen de la protection des données (EDPB) : https://edpb.europa.eu
Autorités nationales chargées de la protection des données : https://edpb.europa.eu/about-edpb/board/members_en

Application de la loi
Réseau d'autorités indépendantes chargées des plaintes à l'encontre des forces de police (IPCAN) : https://ipcan.org/
Agence de l'Union européenne pour la formation des services répressifs (CEPOL) : https://www.cepol.europa.eu/
Agence de l'Union européenne pour la coopération des services répressifs (Europol) : https://www.europol.europa.eu/

Gestion des frontières
Agence européenne de garde-frontières et de garde-côtes (Frontex) : https://frontex.europa.eu/
Bureau européen d'appui en matière d'asile (EASO) : https://www.easo.europa.eu/

Bases de données à grande échelle
Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) : https://www.eulisa.europa.eu/

1 Présentation du contexte : qu'est-ce que le profilage ?

Le présent chapitre décrit ce que l'on entend par profilage et explique les principaux droits fondamentaux qu'il peut affecter. Il présente le profilage dans le contexte des opérations des services de police et de gestion des frontières en examinant trois éléments essentiels :

- la notion de profilage et son utilisation par les services de police et les autorités chargées de la gestion des frontières. Cette section présente également certains des différents types de profilage ;
- les principes les plus importants en matière de droits fondamentaux qui doivent être respectés pour que le profilage soit réalisé dans le respect des lois, à savoir la non-discrimination et les droits au respect de la vie privée et à la protection des données ;
- les incidences négatives potentielles du profilage, y compris les conséquences possibles pour les individus et les relations avec les communautés, ainsi que la confiance dans la police et dans les autorités chargées de la gestion des frontières.

1.1. Définition du profilage

Le profilage consiste à **catégoriser les individus** en fonction de leurs caractéristiques personnelles. Ces caractéristiques peuvent être « immuables » (telles que l'âge ou la taille) ou « modifiables » (telles que les vêtements, les habitudes, les préférences

et d'autres éléments comportementaux). Le profilage inclut l'exploration de données par laquelle les individus sont catégorisés « **sur la base de certaines de leurs caractéristiques observables, afin d'en déduire, avec une certaine marge d'erreur, d'autres qui ne le sont pas** » [3].

Points clés

- Le profilage consiste à **catégoriser les individus** en fonction de leurs caractéristiques déduites.
- Le profilage réalisé dans le contexte des services de police et de la gestion des frontières poursuit deux objectifs principaux : **identifier des personnes connues sur la base de renseignements concernant une personne spécifique** et, à titre de **méthode prédictive**, identifier des personnes « inconnues » susceptibles d'intéresser les autorités répressives et les autorités chargées de la gestion des frontières. Les deux peuvent inclure des préjugés conscients ou inconscients susceptibles d'avoir un effet discriminatoire à l'égard de certains individus.
- Les activités de profilage des gardes-frontières et des agents de police peuvent être influencées par des préjugés induits par leurs expériences individuelles ou institutionnelles. Ces préjugés peuvent alimenter et modifier l'évaluation du profilage, affectant à la fois la légalité et l'efficacité des activités de police.
- Les stéréotypes peuvent refléter une certaine vérité statistique. Toutefois, même dans ces cas, ils **demeurent problématiques** s'ils ont pour conséquence de traiter une personne sur la base de son appartenance à un groupe et non pas sur la base de sa situation individuelle.
- Lors de l'élaboration et de l'utilisation du profilage algorithmique, des **partis pris peuvent être introduits à chaque étape du processus**. Afin d'éviter des violations potentielles des droits fondamentaux à ce stade et ultérieurement, les experts informatiques qui conçoivent les algorithmes et les agents chargés de la collecte et de l'interprétation des données doivent avoir une bonne compréhension des droits fondamentaux et des modalités de leur application dans ce contexte.

Les pratiques de profilage sont utilisées pour :

- générer des connaissances, en analysant les données existantes afin de formuler des hypothèses sur un individu. Les expériences passées et les analyses statistiques sont utilisées pour établir des corrélations entre certaines caractéristiques et certains résultats ou comportements particuliers ;

3 Dinant, J.-M., Lazaro, C., Poullet, Y., Lefever, N. et Rouvroy, A. (2008), p. 3.

- soutenir les processus décisionnels, en utilisant ces corrélations pour prendre des décisions sur les mesures à mettre en place.

Cela fait du profilage un outil puissant pour les agents de police et les gardes-frontières. Toutefois, il comporte des risques importants :

- le profilage établit des corrélations générales qui peuvent ne pas être valables pour chaque individu. Toute personne peut être l'« exception à la règle » ;

- les profils peuvent générer des corrélations incorrectes, tant pour des personnes spécifiques que pour des groupes ;

- les profils peuvent créer des stéréotypes préjudiciables et entraîner une discrimination ;

- certains stéréotypes peuvent refléter une vérité statistique. Toutefois, même dans ces cas, les stéréotypes demeurent problématiques s'ils ont pour conséquence que la personne soit traitée comme un membre d'un groupe plutôt que comme un individu.

Exemples

Profilage potentiellement inexact

L'hypothèse selon laquelle les femmes vivent plus longtemps que les hommes est étayée par une recherche factuelle ; toutefois, tout homme en particulier peut vivre plus longtemps qu'une femme en particulier. Par conséquent, toute prise de décision à l'égard d'une femme sur la base de cette hypothèse risque d'être inexacte dans un cas unique et ne serait valable qu'en moyenne.

Des personnes peuvent autoriser leur famille ou leurs amis à utiliser leur voiture, rendant ainsi peu fiable tout profil de comportement à risque au volant fondé sur la propriété de la voiture.

1.1.1. Profilage dans le contexte de l'application de la loi et de la gestion des frontières

Le **profilage** est communément et légitimement utilisé par les agents de police et les gardes-frontières afin de prévenir les infractions pénales, d'enquêter sur celles-ci et de poursuivre leurs auteurs, ainsi que de prévenir et de détecter l'immigration irrégulière.

Le **profilage** désigne « toute forme de traitement automatisé des données à caractère personnel consistant en l'utilisation de données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique » [4]. Les résultats de ce traitement des données sont utilisés pour orienter les actions en matière de gestion des frontières et d'application de la loi, telles que le contrôle et la fouille, les arrestations, le refus d'accès à certaines zones ou la décision de procéder à des « vérifications de deuxième ligne » plus approfondies à la frontière. Il existe deux grandes utilisations du profilage :

- identifier les individus sur la base de renseignements spécifiques. Cette technique utilise un profil qui énumère les caractéristiques des suspects particuliers, sur la base d'éléments de preuve recueillis au sujet d'un événement donné ;

- en tant que méthode prédictive pour identifier les personnes « inconnues » susceptibles d'intéresser les autorités répressives et les autorités chargées de la gestion des frontières. Elle repose sur une analyse des données et sur des hypothèses fondées sur l'expérience. Idéalement, les méthodes prédictives se concentrent sur le comportement. Dans la pratique, toutefois, l'accent n'est pas souvent (ou pas seulement) mis sur les comportements, mais bien sur des caractéristiques physiques visibles, telles que l'âge, le sexe ou l'origine ethnique.

Le tableau 1 présente une comparaison des caractéristiques essentielles de ces deux types de profilage dans le cadre des activités de police.

4 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 (directive « police »), article 3, paragraphe 4.

Tableau 1 : Caractéristiques des activités de police fondées sur les renseignements spécifiques et de la police prédictive

	Activités de police fondées sur les renseignements spécifiques	Police prédictive
Contexte	Une infraction pénale a été commise, ou un signalement a été introduit concernant une personne en particulier.	Aucune infraction pénale n'a été commise, ou aucun signalement n'a été introduit concernant une personne en particulier.
Approche	Réactive	Proactive
Objectif	Appréhender le(s) suspect(s)	Prévoir où et quand des infractions pénales peuvent se produire ou qui pourrait tenter d'entrer clandestinement dans le pays
Données utilisées	Les renseignements spécifiques relatifs à l'affaire (le « profil individuel »)	Les renseignements génériques relatifs à plusieurs affaires
Type de processus	Les processus axés sur les données et les processus humains sont combinés	Principalement axé sur les données (« analyse des risques »)

Source : FRA (2018).

Les deux types de profilage peuvent être illicites s'ils ne sont pas réalisés dans le respect de garanties spécifiques, y compris l'établissement d'une justification objective et raisonnable du profilage. Les chapitres 2 et 3 fournissent des informations pratiques sur la manière de garantir que le profilage est à la fois légal et conforme aux droits de l'homme.

1.1.2. Définition du profilage algorithmique

L'évolution rapide des technologies implique que le profilage recourt de plus en plus à des données stockées dans des bases de données et dans des systèmes informatiques. Le profilage algorithmique utilise des techniques différentes pour établir des profils sur la base de corrélations et de modèles dans les données. Le profilage algorithmique permet aux agents de police et de la gestion des frontières de cibler des individus ou des groupes spécifiques qui posent un certain risque sur la base de l'analyse des données.

Le profilage algorithmique soulève d'importants problèmes en matière de droits fondamentaux, tels que la discrimination potentielle et les violations des droits au respect de la vie privée et à la protection des données. Cette section du guide se concentre sur la manière dont les services de police et les fonctionnaires chargés

de la gestion des frontières peuvent utiliser et traiter les données dans leur travail quotidien tout en respectant les principes des droits fondamentaux.

Traitement des données à caractère personnel : que dit la loi ?

Les normes juridiques applicables au traitement des données à caractère personnel pour l'établissement des profils sont définies dans le cadre juridique de l'Union en matière de protection des données. Conformément à l'article 4, paragraphe 4, du règlement général sur la protection des données (RGPD) et à l'article 3, paragraphe 4, de la directive « police », « on entend par "profilage", toute forme de traitement automatisé de données à caractère personnel consistant à utiliser des données à caractère personnel pour évaluer certains aspects personnels propres à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

L'article 22, paragraphe 1, du règlement général sur la protection des données dispose que le profilage ne peut être accepté que si la décision n'est pas exclusivement fondée sur un traitement automatique et ne produit pas d'effets sur les personnes susceptibles de les affecter de manière significative.

Le profilage relevant du champ d'application de la directive « police » (voir la section 3.1 sur le profilage algorithmique et la protection des données) doit se conformer à l'article 11, paragraphe 3, de la directive « police ». Il dispose que « [t]out profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 10 * est interdit, conformément au droit de l'Union ».

* Les « catégories particulières de données à caractère personnel » sont des « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant

la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Voir l'article 10, paragraphe 1, de la directive « police ».

La méthode utilisée pour créer des profils pour le profilage algorithmique est similaire à une technique connue sous le nom d'« **analyse comportementale** », dans laquelle des liens sont établis entre certaines caractéristiques et certains modèles de comportement. La figure 1 montre comment des algorithmes peuvent être utilisés pour effectuer des prédictions.

Plein feu sur la manière dont les algorithmes sont utilisés pour étayer la prise de décision

Grâce à l'augmentation de la disponibilité et de l'utilisation des données, la prise de décision est de plus en plus facilitée ou remplacée par des méthodes de modélisation prédictive, souvent appelées « algorithmes ». Un algorithme est une séquence d'instructions permettant à un ordinateur de transformer une entrée en une sortie. De nombreux algorithmes sont basés sur des méthodes statistiques et utilisent des techniques qui calculent les relations entre différentes variables. Par exemple, les données relatives à la consommation d'alcool d'un groupe de personnes et les données sur l'espérance de vie du même groupe peuvent être utilisées ensemble pour calculer l'influence moyenne de la consommation d'alcool sur l'espérance de vie.

La production d'algorithmes est toujours une probabilité, ce qui signifie qu'il existe un degré d'incertitude quant aux relations ou aux classifications qui en découlent. Par exemple, les fournisseurs de courrier électronique utilisent des algorithmes pour identifier quels messages sont des spams et classer ceux-ci comme courrier indésirable. Les algorithmes fonctionnent bien mais ne sont pas parfaits. Il arrive que des spams ne soient pas détectés et finissent dans la boîte de réception ; il s'agit d'un faux négatif (c'est-à-dire un message faussement non identifié en tant que spam). Moins fréquemment, un courrier électronique légitime peut être sélectionné par le filtre antispam et être envoyé dans le répertoire de courrier indésirable : il s'agit là d'un faux positif.

Avoir une compréhension de base de la manière dont les algorithmes soutiennent la prise de décision permet aux professionnels d'identifier et de poser les bonnes questions concernant les problèmes potentiels liés

à l'utilisation d'algorithmes, y compris la possibilité que ceux-ci ne respectent pas les droits à la non-discrimination, au respect de la vie privée ou à la protection des données personnelles des individus.

Pour de plus amples informations, voir FRA (2018b).

La création d'algorithmes de prédiction est un processus complexe qui nécessite de nombreuses prises de décisions par plusieurs personnes impliquées dans ce processus. En tant que tel, le processus ne désigne pas seulement les règles suivies par un ordinateur : il englobe également les phases de collecte, de préparation et d'analyse des données. Il s'agit d'un processus humain qui comprend plusieurs étapes, impliquant des décisions des développeurs et de la direction. La méthode statistique n'est qu'une partie du processus d'élaboration des règles finales utilisées pour la prédiction, la classification ou les décisions [5]. En tout état de cause, la manière dont les données sont collectées et utilisées peut être discriminatoire.

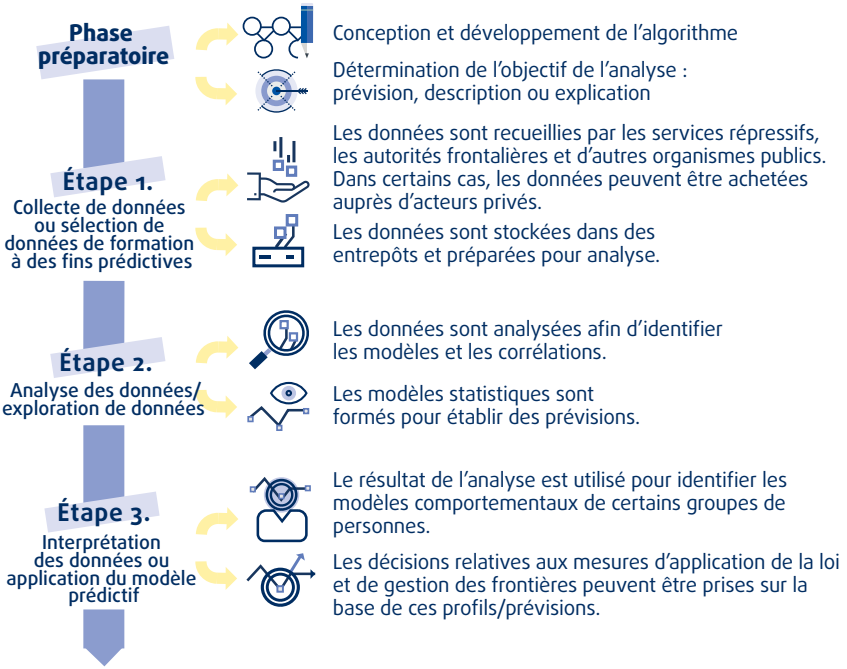
Exemple

Pour être efficaces et précis, les logiciels de reconnaissance faciale doivent être alimentés de quantités massives d'images et de données. Plus ils reçoivent de données, plus leurs résultats seront précis. Toutefois, à ce jour, les images prises en compte dans les algorithmes pour les entraîner sont majoritairement des images d'hommes blancs, avec un nombre relativement faible de femmes et/ou de personnes d'autres origines ethniques. En conséquence, les résultats produits par le logiciel sont moins précis et plus susceptibles d'être inexacts pour les personnes appartenant à ces groupes. Lorsqu'ils sont utilisés par les agents de police ou les gardes-frontières pour établir un profil et pour décider, par exemple, de leur arrestation, les erreurs pouvant découler de ces résultats imprécis peuvent avoir une incidence grave sur les droits et les libertés de la personne.

Pour de plus amples informations, voir Center on Privacy and Technology at Georgetown Law (2016) ; et Buolamwini, J., Gebru, T. (2018).

5 FRA (2018b), p. 4.

Figure 1 : Processus de profilage algorithmique appliqués aux contextes de l'application de la loi et de la gestion des frontières



Source : FRA (2018) [adapté de/fondé sur Perry, W. L., et al. (2013), p. 11–15, et Zarsky, T. Z. (2002–2003), p. 6–18].

Des préjugés peuvent être introduits à chaque étape du processus de profilage algorithmique. Afin d'éviter tout préjugé discriminatoire et des violations des droits à la protection des données et au respect de la vie privée, tant les personnes qui conçoivent les algorithmes que les agents de police et les agents chargés de la gestion des frontières qui collectent et interprètent les données devraient avoir une compréhension claire des droits fondamentaux et de leur application dans ce contexte.

L'utilisation de données fiables est donc essentielle. Dans le cadre du profilage algorithmique, la qualité des données doit être évaluée afin de pouvoir juger de la fiabilité de ces données : moins la qualité varie, et plus elle sera fiable. L'utilisation de données reflétant des préjugés existants ou provenant de sources non vérifiées afin de développer un algorithme produira des résultats biaisés et peu fiables. Enfin, des

erreurs peuvent également se produire durant la phase de prédictions produites par les données. Ainsi :

- les faux positifs désignent des cas où des personnes ont été sélectionnées et soumises à un examen plus approfondi, et ce sur la base d'une prédiction erronée selon laquelle ces personnes représenteraient un risque ;

- les faux négatifs désignent des personnes qui présentent un risque réel dans le cadre des opérations de police et de gestion des frontières, mais qui n'ont pas été identifiées comme telles par le système.

1.2. Quand le profilage est-il illégal ?

Points clés

- Les caractéristiques personnelles peuvent être utilisées comme facteurs légitimes de profilage. Toutefois, afin d'éviter que le profilage ne soit discriminatoire et, par conséquent, illicite, il doit également exister des motifs raisonnables de suspicion fondés sur des informations autres que les **motifs protégés**.
  - Les motifs protégés comprennent le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge et l'orientation sexuelle.
  - Les motifs protégés peuvent être révélés, déduits ou prédits à partir d'autres données à caractère personnel.
- Pour recueillir et traiter les données à **caractère personnel**, les services de police et les autorités chargées de la gestion des frontières doivent veiller à ce que la collecte et le traitement des données aient une base juridique, un objectif valide et légitime et soient nécessaires et proportionnés.
  - Les données à caractère personnel sont des informations qui peuvent être utilisées pour identifier, directement ou indirectement, une personne, telles qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Lorsqu'il est utilisé légalement, le profilage est une **technique d'enquête légitime**. Pour être légal, il doit être fondé sur des **justifications objectives et raisonnables** et respecter les droits fondamentaux, tels que le droit à la non-discrimination et à la protection des données à caractère personnel. Le profilage est considéré comme n'ayant pas de justification objective et raisonnable « s'il ne poursuit pas un objectif légitime ou s'il n'existe pas un rapport raisonnable de proportionnalité entre les moyens utilisés et l'objectif poursuivi » [6].

Lorsque réalisé de manière illégale, le profilage affecte de nombreux droits fondamentaux. Cependant, cette section se concentre sur les droits fondamentaux qui sont principalement affectés par le profilage illicite : les droits à la

6 Commission européenne contre le racisme et l'intolérance (ECRI) (2007), paragraphe 28.

non-discrimination, au respect de la vie privée et à la protection des données. Le profilage est considéré comme illicite lorsque :

- il comprend des actes de traitement de personnes différencié sur la base de motifs protégés qui sont injustifiés (voir la section 1.2.1), ou

- il interfère inutilement avec la vie privée des personnes et/ou n'est pas conforme aux règles relatives au traitement des données à caractère personnel (voir la section 1.2.2).

1.2.1. L'interdiction de la discrimination

Interdiction de la discrimination : que dit la loi ?

« **Est interdite toute discrimination fondée notamment** sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. » *

Article 21 de la Charte des droits fondamentaux de l'Union européenne

« **La jouissance de tout droit prévu par la loi doit être assurée, sans discrimination aucune, fondée notamment** sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation.

Nul ne peut faire l'objet d'une discrimination de la part d'une autorité publique quelle qu'elle soit fondée notamment sur les motifs mentionnés au paragraphe 1. »

Article 1 du protocole n° 12
à la Convention européenne des droits de l'homme

** Il convient de noter que, dans la pratique, de nombreux États membres ont étendu la protection contre la discrimination au-delà des motifs énumérés dans la Charte et dans la Convention européenne des droits de l'homme (CEDH).*

Il y a discrimination « lorsqu'une personne est traitée de manière moins favorable qu'une autre ne l'est, ne l'a été ou ne le serait dans une situation comparable » sur la base d'une caractéristique personnelle perçue ou réelle [7]. Ces caractéristiques sont appelées « motifs protégés » ou « caractéristiques protégées » dans le droit antidiscrimination. De plus amples informations sur le droit européen et la jurisprudence dans le domaine de la non-discrimination sont disponibles dans l'édition 2018 du *Manuel de droit européen en matière de non-discrimination*, publié conjointement par l'Agence des droits fondamentaux de l'Union européenne et le Conseil de l'Europe [8].

Il existe plusieurs types de discrimination :

Il y a **discrimination directe** lorsqu'une personne est traitée de façon moins favorable, *uniquement ou principalement* parce qu'elle présente un certain motif protégé tel que la race, le sexe, l'âge, le handicap ou l'origine ethnique [9].

Exemple

En réponse à une menace terroriste, la police est habilitée à contrôler et à fouiller toute personne qui, selon elle, pourrait être impliquée dans cette menace. Les services de police pensent que cette menace provient d'une organisation terroriste active dans une certaine région du monde, mais ne possèdent pas d'autre renseignement spécifique. Si un officier de police arrête un homme uniquement ou principalement parce que son apparence indique qu'il peut provenir de la même région du monde, cela constituerait une discrimination directe et serait illégal.

Il y a **discrimination indirecte** (également appelée « discrimination ayant un effet disproportionné » dans le contexte de l'application de la loi et de la gestion des frontières) lorsqu'une disposition, un critère ou une pratique *apparemment neutre* est susceptible d'entraîner un désavantage particulier pour des personnes présentant des caractéristiques protégées particulières par rapport à d'autres personnes,

7 Directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, JO L 180, article 2, et directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail, JO L 303, article 2.

8 FRA et Conseil de l'Europe (2018).

9 Ibid., p. 43.

à moins que cette disposition, ce critère ou cette pratique ne soit objectivement justifié par un objectif légitime et que les moyens de réaliser cet objectif soient nécessaires et proportionnés [10]. La discrimination indirecte requiert généralement des statistiques permettant de déterminer si une personne a été, dans la pratique, traitée moins favorablement qu'une autre sur la base de son appartenance à un groupe présentant des caractéristiques protégées particulières.

Exemple

Pour les contrôles de routine, les autorités répressives décident d'arrêter une voiture sur dix dans la ville X entre 21 heures et 1 heure du matin ; 60 % de la population de la ville X conduisant à cette heure sont d'origine afro-caribéenne, tandis que la population afro-caribéenne de la ville et de la périphérie ne dépasse pas 30 %. Ce groupe étant susceptible d'être plus touché que d'autres, cela équivaudrait à une discrimination indirecte.

Aborder la discrimination sous l'angle d'un seul motif ne permet pas d'appréhender les différentes manifestations de l'inégalité de traitement de façon adéquate. La **discrimination multiple** désigne une discrimination dans laquelle plusieurs motifs agissent séparément. Par exemple, une personne peut être victime de discrimination non seulement en raison de son origine ethnique, mais aussi de son âge et de son sexe [11]. La **discrimination intersectionnelle** désigne une situation où plusieurs motifs agissent et interagissent les uns avec les autres en même temps, d'une manière telle qu'ils sont inséparables et donnent lieu à des types de discrimination particuliers (voir l'exemple dans l'encadré).

Exemple

Un officier de police contrôle et fouille un jeune homme d'origine africaine sans aucune bonne raison de soupçonner qu'il a commis un crime. Ce jeune homme fait l'objet d'une discrimination qui n'est pas uniquement fondée sur son âge (tous les jeunes ne sont pas contrôlés) ou son origine ethnique

10 Directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail, JO L 303 (directive sur l'égalité en matière d'emploi), article 2 ; voir également FRA et Conseil de l'Europe (2018), p. 53.

11 FRA et Conseil de l'Europe (2018), p. 59.

(toutes les personnes d'origine africaine ne sont pas contrôlées), mais précisément sur le fait qu'il est à la fois jeune et d'origine africaine.

La discrimination peut également résulter du traitement automatisé des données à caractère personnel et du recours au profilage algorithmique. La discrimination peut survenir lors de la conception et de la mise en œuvre des algorithmes, par l'intermédiaire de préjugés qui sont incorporés — sciemment ou non — dans l'algorithme, et lorsque les décisions sont prises sur la base des informations obtenues.

L'article 9, paragraphe 1, du RGPD dispose expressément que le traitement de catégories particulières de données à caractère personnel qui révèlent des caractéristiques personnelles, telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, est interdit (se référer à la figure 9 de la section 2.2.4 pour la liste complète des motifs protégés). Cette interdiction peut être levée dans des cas spécifiques, tels que la protection de l'intérêt public, à condition que l'exemption ait une base juridique, soit proportionnée et nécessaire, et prévoie des garanties adéquates [12].

De même, dans le cadre de la prévention, de l'enquête, de la détection et des poursuites concernant des infractions pénales, l'article 11, paragraphe 3, de la directive « police » relatif à la prise de décision individuelle automatisée interdit le « profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel », y compris les données révélant l'origine raciale ou ethnique et les croyances religieuses, ainsi que les données génétiques et biométriques [13]. Une fois encore, des exceptions à cette interdiction sont autorisées dans certains cas, mais doivent être nécessaires, présenter des garanties appropriées, et soit avoir une base juridique, soit avoir pour objectif de protéger les intérêts vitaux d'une personne [14].

12 Règlement général sur la protection des données (RGPD), article 9, paragraphe 2, point g).

13 Pour de plus amples informations, voir le groupe de travail « article 29 » sur la protection des données (2017b).

14 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 (directive « police »), article 10.

Interdiction du profilage discriminatoire : que dit la loi ?

« **Tout profilage qui entraîne une discrimination** à l'égard de personnes physiques sur **la base de données à caractère personnel** qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, **devrait être interdit** en application des conditions établies aux articles 21 et 52 de la Charte [des droits fondamentaux]. »

Considérant 38 de la directive « police ».

« **Tout profilage qui entraîne une discrimination** à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 10 * **est interdit**, conformément au droit de l'Union. »

Article 11, paragraphe 3, de la directive « police ».

** Article 10 de la directive « police » : « données [...] qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».*

« Lors des vérifications aux frontières, les gardes-frontières **n'exercent envers les personnes aucune discrimination** fondée sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, un handicap, l'âge ou l'orientation sexuelle. »

Article 6 du code frontières Schengen

L'interdiction de la discrimination ne signifie pas que les caractéristiques personnelles ne peuvent être utilisées comme facteurs légitimes de profilage dans le cadre d'enquêtes pénales ou de vérifications aux frontières (voir la section 2.3). Toutefois, il doit exister des motifs raisonnables de suspicion fondés sur des informations autres que les motifs protégés. Par exemple, une personne peut correspondre à une description spécifique d'un suspect ou son apparence peut ne pas correspondre aux informations contenues dans son document de voyage [15].

15 Royaume-Uni, House of Lords (2006), Lord Scott, Opinions of the Lords of appeal for judgment in *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.*, [2006] UKHL 12, 8 mars 2006, paragraphe 67.

Plein feu sur la discrimination fondée sur la nationalité

L'article 21 de la Charte des droits fondamentaux de l'Union européenne **limite l'interdiction de toute discrimination fondée sur la nationalité aux citoyens de l'Union**. Dans la directive sur l'égalité raciale, la nationalité ne fait pas partie des motifs protégés.

Toutefois, les États membres ont élargi le champ d'application de l'interdiction de la discrimination pour couvrir la nationalité de différentes manières. Il s'agit notamment de reconnaître que la nationalité est parfois utilisée comme une valeur de substitution de la race, de l'origine ethnique ou de la religion. Dans certains cas, « des différences de traitement fondées sur la nationalité [...] [seront] constatées en violation de la législation interdisant la discrimination fondée sur ces motifs » (voir le Réseau européen d'experts juridiques dans le domaine de l'égalité des genres et de la non-discrimination, 2016, p. 99). Dans la pratique, la discrimination fondée sur la nationalité et la discrimination fondée sur l'appartenance ethnique sont souvent difficiles à distinguer.

Le fait que la nationalité ne soit pas explicitement mentionnée comme étant un motif de discrimination potentiel à l'article 21 de la Charte reflète principalement le statut différent des citoyens de l'Union (et des autres personnes jouissant du droit à la libre circulation en vertu du droit de l'UE) et des ressortissants de pays tiers en vertu du droit de l'UE. Cet aspect revêt une importance particulière dans les procédures à la frontière, où la nationalité est le facteur décisif pour déterminer si une personne fera l'objet d'une vérification approfondie, ou si elle doit être en possession d'un visa pour entrer dans l'espace Schengen ou transiter par celui-ci.

Dans le même temps, le renvoi systématique de toutes les personnes d'une nationalité spécifique vers les vérifications de deuxième ligne risque de devenir discriminatoire. La nationalité peut être un élément légitime des profils de risque pour détecter la migration irrégulière ou les victimes présumées de la traite des êtres humains, mais elle ne doit pas être l'unique ou principal déclencheur d'une vérification de deuxième ligne. En outre, comme dans d'autres contextes, le traitement différencié fondé sur la nationalité devient discriminatoire et donc illicite lorsqu'il est utilisé indirectement pour discriminer sur la base de motifs protégés étroitement liés à la nationalité, tels que la race, l'origine ethnique ou la religion.

Dans ses Principes et directives recommandés sur les droits de l'homme aux frontières internationales de 2014, le Haut Commissariat des Nations unies aux droits de l'homme inclut la nationalité parmi les motifs protégés qui ne devraient pas être utilisés pour le profilage des migrants (principe 8).

Jurisprudence

Dans l'affaire *Rosalind Williams Lecraft c. Espagne*, une femme a été arrêtée sur le quai d'une gare en Espagne par un officier de police qui lui a demandé de lui présenter ses papiers d'identité. La femme a demandé au policier pour quelle raison elle était la seule personne contrôlée sur le quai et il lui a répondu : « C'est parce que vous êtes noire ». Dans sa décision, le Comité des droits de l'homme des Nations unies a souligné qu'il était généralement légitime d'effectuer des contrôles d'identité dans l'intérêt de la sécurité publique ainsi que de prévenir la criminalité et de surveiller l'immigration irrégulière. Toutefois, il a constaté que « lorsque les autorités se livrent à ces contrôles, les caractéristiques physiques ou ethniques des personnes qui en sont l'objet ne doivent pas être considérées comme des indices de leur possible présence illégale dans le pays. Ces contrôles d'identité ne doivent pas non plus être effectués de telle sorte que seules les personnes ayant certaines caractéristiques physiques ou ethniques soient visées. Cela aurait non seulement des répercussions négatives en termes de dignité des personnes concernées mais contribuerait également à propager des attitudes xénophobes dans la population en général et serait contraire à une politique effective de lutte contre la discrimination raciale ».

En 2017, une plainte similaire a été déposée auprès de la Cour européenne des droits de l'homme, concernant le traitement d'un ressortissant pakistanais pendant et après un contrôle de police en Espagne. Le tribunal devra décider si le plaignant a fait l'objet d'une discrimination fondée sur l'origine ethnique lors du contrôle d'identité et s'il y a eu violation de l'article 8 (droit à la vie privée et familiale) du fait que les autorités espagnoles n'ont pas pris toutes les mesures raisonnables pour corriger d'éventuels motifs racistes. Le jugement est en cours au moment de la rédaction du présent document.

Pour de plus amples informations, voir HCR, Rosalind Williams Lecraft c. Espagne*, Comm. n° 1493/2006 et Cour européenne des droits de l'homme,*

Zeshan Muhammad c. Spain, *nº 34085/17, déposée le 6 mai 2017. Voir également FRA et Conseil de l'Europe (2018).*

Dans l'affaire *B.S. c. Espagne*, une prostituée d'origine nigériane résidant légalement en Espagne alléguait que la police espagnole l'avait maltraitée physiquement et verbalement en raison de sa race, de son genre et de sa profession. Elle soutenait que, contrairement aux autres prostituées d'origine européenne, elle avait fait l'objet de contrôles de police répétés et qu'elle avait été victime d'insultes racistes et sexistes. Deux interventions de tiers du Centre AIRE et de l'unité de recherche sociale européenne de l'université de Barcelone ont demandé à la CouEDH de reconnaître la discrimination intersectionnelle. La Cour a constaté une violation de l'article 3 (interdiction des traitements inhumains et dégradants), mais a continué à examiner séparément s'il y avait également manquement à l'obligation d'enquêter sur un éventuel lien de causalité entre les attitudes racistes alléguées et les actes de violence de la police. Sur ce point, la CouEDH a constaté une violation de l'article 14 (interdiction de la discrimination), parce que les tribunaux nationaux n'avaient pas tenu compte de la vulnérabilité particulière de la requérante en tant que femme africaine travaillant comme prostituée. Bien qu'il adopte une approche intersectionnelle, l'arrêt n'a pas utilisé le terme « intersectionnalité ».

Pour de plus amples informations, voir Cour européenne des droits de l'homme, B.S. c. Espagne*, nº 47159/08, 24 juillet 2012.*

Plein feu sur la charge de la preuve

En 2016, la Cour de cassation française a statué pour la première fois sur la question des contrôles d'identité discriminatoires. Dans ses arrêts du 9 novembre 2016, la Cour a jugé que la police avait procédé à des contrôles d'identité discriminatoires sur trois des 13 hommes d'origine africaine ou nord-africaine. La responsabilité de l'État a été retenue dans ces affaires et la Cour l'a condamné à verser des dommages-intérêts aux trois requérants. Dans huit autres affaires, la Cour a jugé que les contrôles d'identité contestés étaient légaux puisqu'ils étaient fondés sur des éléments objectifs et, partant, non discriminatoires. Les juges n'ont pas statué sur les deux autres affaires, les renvoyant aux juridictions inférieures pour révision.

La Cour a également clarifié la charge de la preuve dans pareils cas. Les contrôles d'identité ne sont pas enregistrés lorsqu'ils ne donnent pas lieu à des procédures judiciaires ou administratives. La Cour a expliqué que les requérants doivent apporter au juge des éléments de preuve qui laissent présumer l'existence d'une discrimination. La police doit prouver soit l'absence de traitement différencié dans la mise en œuvre des contrôles d'identité, soit une différence de traitement justifiée par des éléments objectifs.

En outre, la Cour a estimé que les juges pouvaient prendre en compte, comme preuves, des études et des informations statistiques attestant la fréquence des contrôles d'identité effectués, pour des motifs discriminatoires, sur une même catégorie de population que le requérant (à savoir les minorités visibles, déterminées par des caractéristiques physiques résultant de l'origine réelle ou supposée). Toutefois, ces preuves ne suffisent pas, à elles seules, à suggérer une discrimination.

Par conséquent, la Cour a considéré qu'un contrôle d'identité fondé sur des caractéristiques physiques liées à une origine ethnique réelle ou supposée, sans justification objective préalable, est discriminatoire et constitue une faute grave qui, dans ces trois cas, engageait la responsabilité de l'État.

Pour de plus amples informations, voir France, Cour de cassation, arrêt nº 1245, 9 novembre 2016.

1.2.2. Le droit au respect de la vie privée et à la protection des données à caractère personnel

En vertu du droit de l'UE, le droit au respect de la vie privée (article 7 de la Charte) et à la protection des données à caractère personnel (article 8 de la Charte) sont des droits distincts, mais étroitement liés. Le droit à la vie privée est un droit plus vaste qui interdit *toute ingérence* dans la vie privée d'un individu. La vie privée ne se limite pas aux éléments que l'on souhaite garder confidentiels, mais aussi aux moyens par lesquels une personne exprime sa personnalité, par exemple en choisissant ses fréquentations ou un style vestimentaire. La protection des données à caractère personnel se limite à l'appréciation de la légalité en ce qui concerne le *traitement des*

données à caractère personnel [16]. Les deux droits sont utilisés indifféremment aux fins du présent guide en l'absence de référence spécifique au droit de l'Union. Ces droits ne sont pas absolus et peuvent être limités dans certaines circonstances (voir l'article 8 de la CEDH et l'article 52 de la Charte).

Droits à la vie privée et à la protection des données à caractère personnel : que dit la loi ?

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Article 8 de la Convention européenne des droits de l'homme

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

Article 7 de la Charte des droits fondamentaux de l'Union européenne

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. [...] »

Article 8 de la Charte des droits fondamentaux de l'Union européenne

« 1. La personne concernée a le droit de ne pas faire l'objet d'une décision **fondée exclusivement sur un traitement automatisé**, y compris le profilage, **produisant des effets juridiques** la concernant **ou l'affectant de manière significative** de façon similaire.

2. Le paragraphe 1 ne s'applique pas lorsque la décision :

16 FRA, CEPD et Conseil de l'Europe (2018).

a) est nécessaire à la conclusion ou à l'exécution d'un contrat [...] ;

b) est autorisée par le droit [...] qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ;

c) est fondée sur le consentement explicite de la personne concernée. »

Article 22, paragraphes 1 et 2, du règlement général sur la protection des données

« Les États membres prévoient que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis et qui fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement. »

Article 11, paragraphe 1, de la directive « police »

Le droit dérivé de l'UE précise les droits à la vie privée et à la protection des données à caractère personnel. Deux actes législatifs spécifient la manière dont les données à caractère personnel peuvent être collectées et traitées. Le règlement (UE) 2016/679, à savoir le règlement général sur la protection des données (RGPD), énonce des principes généraux et des garanties concernant le traitement des données à caractère personnel. Plus précisément, la directive 2016/680, dite directive « police », établit les règles applicables au traitement des données à caractère personnel dans le cadre des opérations de répression à des fins de prévention et de détection des infractions pénales, ainsi que d'enquêtes et de poursuites en la matière. Les principes les plus importants et certaines différences essentielles entre les deux sont illustrés dans le tableau 2. Les lois établissant les grandes bases de données de l'UE utilisées pour la gestion des frontières, telles que le système d'information sur les visas (VIS), le système d'entrée/sortie (EES) ou le système européen d'information et d'autorisation concernant les voyages (ETIAS), contiennent également chacune un cadre spécifique pour la protection des données (voir section 3.2 sur les bases de données à grande échelle).

Tableau 2 : Exigences en matière de protection des données : différences entre la directive « police » et le RGPD

Principe de protection des données	RGPD	Directive « police »
Licéité, loyauté, transparence	Tout traitement de données à caractère personnel doit être licite, loyal et **transparent**.	Les données à caractère personnel doivent être traitées loyalement et licitement.
Limitation de la finalité	Les données à caractère personnel collectées pour une finalité déterminée ne devraient pas être traitées ultérieurement à des fins incompatibles ; **le traitement ultérieur à des fins scientifiques, statistiques ou historiques ne sera pas considéré comme incompatible avec les finalités initiales**.	Les données à caractère personnel collectées pour une finalité déterminée ne devraient pas être traitées ultérieurement à des fins incompatibles ; les autres finalités ne seront pas incompatibles avec la finalité initiale si ce traitement est autorisé par la loi et est nécessaire et proportionné.
Minimisation des données	Les données à caractère personnel collectées sont adéquates, pertinentes et **limitées à ce qui est nécessaire** pour les finalités pour lesquelles elles ont été collectées.	Les données à caractère personnel doivent être adéquates, pertinentes et **non excessives** au regard des finalités pour lesquelles elles ont été collectées.
Limitation de la conservation	Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles ont été collectées ; **les données à caractère personnel peuvent être conservées pour des durées plus longues à des fins de recherche scientifique ou historique ou à des fins statistiques**.	Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles ont été collectées.
Exactitude	Les données à caractère personnel collectées doivent être exactes et tenues à jour. Les données à caractère personnel incorrectes ou inexactes doivent être effacées ou rectifiées.	
Intégrité et confidentialité	Les données à caractère personnel doivent être protégées contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.	

Source : FRA (2018).

Exemples

Un garde-frontière envoie la liste des passagers d'un avion à des personnes non autorisées. Une fois partagées, ces données à caractère personnel peuvent être utilisées à des fins autres et/ou privées. Il s'agit d'une violation manifeste des principes de protection des données.

Un officier de police quitte son bureau en laissant une liste de données à caractère personnel relatives à des suspects affichée sur son écran d'ordinateur. En sapant le principe de sécurité des données à caractère personnel, il commet une violation des principes de protection des données.

Jurisprudence

Les arrêts de la Cour donnent des orientations sur la manière dont ces principes sont appliqués dans la pratique.

Limitation de la finalité

Dans l'affaire *Heinz Huber c. Bundesrepublik Deutschland,* la CJUE a évalué la légitimité du registre central allemand des étrangers (*Auslanderzentralregister, AZR*), qui contient certaines données à caractère personnel relatives aux ressortissants étrangers — citoyens de l'UE et ressortissants de pays tiers — qui résident en Allemagne pendant plus de trois mois. La CJUE a conclu que les données collectées pour une finalité spécifique ne pouvaient pas être utilisées à des fins différentes. La Cour a estimé que l'AZR était un instrument légitime pour appliquer les règles de résidence et que la différence de traitement entre les ressortissants étrangers et les ressortissants allemands, pour lesquels moins de données sont conservées, est justifiée compte tenu de l'objectif poursuivi. Toutefois, la CJUE a estimé que les données stockées dans l'AZR ne pouvaient pas être utilisées pour lutter contre la criminalité en général, étant donné qu'il s'agit d'une finalité différente de celle pour laquelle les données ont été initialement collectées.

Pour de plus amples informations, voir CJUE, affaire C-524/06, Heinz Huber c. Bundesrepublik Deutschland, *16 décembre 2008.*

Limitation de la conservation

Dans l'affaire *S. et Marper c. Royaume-Uni,* les requérants ont demandé la suppression de leurs relevés (empreintes digitales, échantillons cellulaires et profils ADN) de la base de données ADN utilisée pour l'identification criminelle au Royaume-Uni. Leurs procès se sont soldés par un acquittement et ils s'inquiétaient des éventuelles utilisations actuelles et futures de leurs données. La police a refusé. La CouEDH a conclu que la conservation illimitée des échantillons d'ADN des personnes qui sont arrêtées, mais acquittées par la suite, ou qui font l'objet d'une décision de classement sans suite, constitue une atteinte au droit à la vie privée. La Cour a souligné le risque de stigmatisation, étant donné que les données des personnes qui n'avaient pas été condamnées pour une infraction étaient traitées de la même manière que celles des personnes condamnées. La Cour a également reconnu que la conservation de telles données peut être particulièrement préjudiciable dans le cas de mineurs, en raison de l'importance que revêt leur développement et leur intégration dans la société.

Pour de plus amples informations, voir Cour européenne des droits de l'homme, S. et Marper c. Royaume-Uni, *n^os^ 30562/04 et 30566/04, 4 décembre 2008.*

Afin de recueillir et de traiter des données à caractère personnel à des fins de profilage, les services de police et les autorités chargées de la gestion des frontières doivent respecter quatre critères juridiques essentiels. La collecte et le traitement des données doivent :

- **être définis et régis par la loi** (***base juridique***) : toute limitation des droits au respect de la vie privée et à la protection des données doit être prévue par la loi et respecter le contenu essentiel de ces droits. La loi doit se conformer aux critères de clarté et de qualité, ce qui signifie que le public y a accès et qu'elle est suffisamment claire et précise pour permettre au public de comprendre son application et ses conséquences ;

- **avoir une finalité valable, légale et appropriée (*objectif légitime*) :** les objectifs légitimes sont fixés par la loi et ne peuvent être étendus. Ils peuvent porter sur la sécurité nationale, la santé, l'ordre public ou la prévention de la criminalité ;

- **être indispensables à la réalisation de cet objectif (*nécessité*) :** le traitement des données à caractère personnel devrait être limité à ce qui est nécessaire pour la finalité pour laquelle les données ont été collectées ;

- **ne pas être excessifs (*proportionnalité*) :** les autorités qui traitent des données à caractère personnel devraient parvenir à un juste équilibre entre la finalité et les moyens utilisés pour y parvenir. En d'autres termes, la valeur ajoutée du traitement ne devrait pas l'emporter sur son impact négatif potentiel.

Le chapitre 3 explique comment ces principes peuvent être appliqués dans la pratique.

La figure 2 montre comment ces principes peuvent être utilisés pour déterminer si une action est susceptible de porter atteinte aux droits au respect de la vie privée et familiale et à la protection des données (voir également la section 2.3.3 sur les mécanismes de plainte). L'affaire *Gillan et Quinton c. Royaume-Uni* sur les opérations de contrôle et de fouille illustre la manière dont la Cour européenne des droits de l'homme a appliqué ces principes pour déterminer s'il y avait eu violation du droit à la protection des données et au respect de la vie privée (voir l'encadré sur la jurisprudence).

Figure 2 : Atteinte à la vie privée et à la protection des données — Le processus d'évaluation

Source : FRA (2018) [basé sur le Conseil de l'Europe (2003), Le droit au respect de la vie privée et familiale : un guide sur la mise en œuvre de l'article 8 de la Convention européenne des droits de l'homme].

Jurisprudence

Dans l'affaire *Gillan et Quinton c. Royaume-Uni*, les requérants, deux ressortissants britanniques, ont cherché à contester la légalité des pouvoirs de contrôle et de fouille utilisés à leur encontre par voie de contrôle juridictionnel.

La mesure adoptée est-elle prescrite par la loi ? La mesure était conforme aux articles 44 à 47 du *Terrorism Act 2000*, qui disposent que : 1) pour la prévention des actes de terrorisme, les officiers de police de rang élevé peuvent autoriser tout officier de police en uniforme à procéder à une interpellation et une fouille dans une zone spécifique ; 2) les autorisations doivent être confirmées par le secrétaire d'État et sont assorties d'une

échéance mais peuvent être renouvelées indéfiniment ; 3) bien que la finalité des fouilles soit de trouver des objets pouvant être utilisés pour des actes de terrorisme, les interpellations et fouilles ne doivent pas être basées sur la suspicion que la (les) personne(s) interpellée(s) détien(nen)t des objets de ce type ; et 4) les personnes refusant de se soumettre à la fouille sont passibles d'emprisonnement, d'une amende, ou des deux (*Gillan et Quinton*, paragraphes 76 à 80).

La mesure adoptée constitue-t-elle une ingérence dans l'exercice du droit au respect de la vie privée et/ou la protection des données ? Le recours à des pouvoirs coercitifs par les autorités répressives pour imposer à quiconque de se plier à une fouille de sa personne, de ses vêtements ou de ses effets personnels est manifestement constitutif d'une ingérence dans l'exercice du droit au respect de la vie privée. L'exposition d'éléments de nature personnelle lors de la fouille aggrave ladite ingérence du fait de l'humiliation et de la gêne qui en résultent (*Gillan et Quinton*, paragraphe 63).

Évaluation de la proportionnalité et de la nécessité : la Cour a exprimé un certain nombre de préoccupations quant à la proportionnalité et à la nécessité de la loi (*Gillan et Quinton*, paragraphes 80 à 86) :

- la norme légale pour l'autorisation des contrôles n'était pas contraignante ;
- l'étendue des pouvoirs statutaires est telle que le justiciable qui cherchera à démontrer qu'une autorisation ou une confirmation a été donnée en excès ou qu'un abus de pouvoir a été commis sera confronté à de formidables obstacles ;
- les zones géographiques couvertes par l'autorisation étaient très larges et le délai a été prolongé à plusieurs reprises, ce qui a réduit le caractère ciblé de l'autorisation ;
- les restrictions imposées à la discrétion des fonctionnaires ont été plus formelles que substantielles ;
- il n'y avait guère de perspective de contrôle judiciaire car, le policier n'étant pas tenu de démontrer l'existence de soupçons légitimes, il était pratiquement impossible de prouver l'abus de pouvoir.

Ces considérations ont amené la CouEDH à conclure que les articles pertinents du *Terrorism Act* n'étaient « ni suffisamment encadrés ni entourés de

garanties légales adéquates contre les abus » et enfreignaient donc l'article 8 de la Convention.

Pour de plus amples informations, voir Cour européenne des droits de l'homme, Gillan et Quinton c. Royaume-Uni, *n° 4158/05, 12 janvier 2010.*

Les exigences juridiques relatives au profilage énoncées dans le cadre juridique réformé de l'UE en matière de protection des données sont détaillées au chapitre 3.

1.3. Quelles sont les incidences négatives potentielles d'un profilage illicite à des fins répressives et de gestion des frontières ?

Le profilage fondé uniquement sur de vastes catégories, telles que la race, l'origine ethnique ou la religion, est non seulement illicite mais peut aussi présenter des inconvénients pour l'efficacité de la police et des autorités chargées de la gestion des frontières. Cette section examine deux incidences négatives potentielles :

- la principale difficulté réside dans la pression qu'il peut exercer sur les relations avec les communautés. Le profilage peut créer un ressentiment parmi les communautés particulièrement touchées et saper la confiance dans la police et les autorités chargées de la gestion des frontières. Cette situation peut à son tour nuire à l'efficacité des méthodes reposant sur la coopération publique ;

- l'efficacité de l'utilisation de grandes catégories de profils dans le cadre de la gestion des frontières ou de l'application de la loi pose également question, par exemple si le profilage en question aboutit à ce qu'une personne fasse l'objet de soupçons injustifiés [17].

En outre, lorsque le profilage est mené de manière illicite, les autorités seront la cible de procédures de plainte ou d'actions en justice. Cela peut prendre la forme d'un contrôle interne par l'intermédiaire de l'office des plaintes de la police, des organismes spécialisés dans les plaintes, des autorités de surveillance ou du système

17 FRA (2017d), p. 51.

judiciaire civil et pénal (voir la section 2.3). Les fonctionnaires et les gestionnaires de niveau intermédiaire peuvent faire l'objet de sanctions administratives et/ou pénales en raison de leur implication dans le profilage illicite ou de leur tolérance vis-à-vis de celui-ci. Cela peut représenter une lourde charge sur les ressources et nuire au moral et à la réputation des autorités.

Points clés

- **Le profilage illicite sape la confiance** dans les autorités de police et de gestion des frontières et peut engendrer une détérioration des relations avec les communautés locales.
- **Il existe des doutes quant à l'efficacité réelle d'un recours intensif au profilage** dans les cadres de la détection de la criminalité ou de la gestion des frontières. Les éléments de preuve ne permettent pas de déterminer si un tel profilage augmente le taux de réussite des opérations de police ou de gestion des frontières.

1.3.1. Impacts du profilage illicite quant à la confiance des individus envers la police et les gardes-frontières et sur la cohésion sociale

Plusieurs travaux de recherche ont démontré l'impact négatif que le recours au profilage peut avoir sur les individus et leurs communautés [18]. L'encadré ci-dessous rend compte des réponses formulées par certains individus après avoir fait l'objet d'un contrôle et d'une fouille, ou lors d'une vérification aux frontières.

Exemples

Impacts des mesures de contrôle et de fouille et des vérifications aux frontières sur les personnes

1. Contrôles policiers — Keskinen, S., et al. (2018)

Entre 2015 et 2017, l'École suédoise des sciences sociales de l'université d'Helsinki a interrogé 185 personnes sur leurs expériences en matière de profilage ethnique. La recherche a indiqué que la plupart des répondants ont

18 FRA (2017d).

jugé les contrôles désagréables, dérangeants ou humiliants. Voici quelques extraits des témoignages des répondants.

« *Un peu plus tard, un autre policier m'a à nouveau interpellée […], tandis que j'étais en train de marcher en rue avec deux amis blancs : un Finlandais et un Néerlandais. Et j'ai fait exactement la même chose… j'ai posé la même question. J'étais fâchée parce que je ne savais pas pourquoi j'avais été sélectionnée. Je leur ai demandé et ils ont simplement répondu qu'ils faisaient leur travail.* » *(Femme, la trentaine, origine africaine)*

« *Une fois, ma mère et mon frère se promenaient en ville ; les policiers les ont arrêtés et ont dit "Passeports, s'il vous plaît". J'appelle ça du profilage ethnique. Puis mon frère [a déclaré en finnois] "Nous n'avons pas nos passeports, nous ne les emportons pas avec nous à chaque fois". Lorsqu'ils se sont rendu compte qu'il parlait couramment le finnois, ils ont répondu "Oh pas de problème". J'étais furieuse parce que je sais que le profilage ethnique est illégal, mais ma mère et mon frère ne le savaient pas. J'ai donc eu l'impression, vous voyez, qu'ils avaient été maltraités. Donc j'étais très en colère. Lorsque je leur ai dit que ce qui leur était arrivé était illégal, ils ont évidemment compris qu'ils avaient été interpellés parce qu'ils […] ne ressemblaient pas à des Finlandais, mais à des étrangers.* » *(Femme, la vingtaine, Finno-Somalienne)*

« *C'est toujours la même description à chaque fois. J'ai presque envie de leur dire, donc pendant 11 ans, vous avez recherché la même personne, qui a réussi à vous échapper pendant tout ce temps ? Vous ne faites pas du bon boulot, alors, car la description que vous [autorité de gestion des frontières] avez est toujours la même, et je corresponds toujours à cette description [rires].* » (Homme, environ 30 ans, pays africain-Finlande)

Pour de plus amples informations, voir Keskinen, S., et al. (2018), The stopped — Ethnic profiling in Finland.

2. Vérifications aux frontières — FRA (2014a et 2014b)

« *Je comprends la raison pour laquelle [le garde-frontière] m'a contrôlé mais il n'avait pas à m'envoyer ici [vérification de deuxième ligne/poste de police] ni à me traiter comme un criminel. Ils font ça avec tous les Européens de l'Est.* » *(Passager de Serbie, homme, interrogé à l'aéroport de Francfort)*

Question : « *Que pensez-vous du traitement dont vous avez fait l'objet lors de la vérification de première ligne ?* »

Réponse : « *Je trouve que ce n'était pas correct. C'était humiliant. Il ne m'a pas bien traité. Il a juste pris mon passeport, l'a regardé puis il s'est contenté d'appeler l'immigration. Il a posé des questions et haussé le ton, mais je n'ai rien compris. Ils m'ont sorti de la ligne mais ils ne m'ont pas respecté et ils m'ont fait peur.* »

Q : « *Pourquoi avez-vous eu peur ou vous êtes-vous senti humilié ?* »

R : « *Parce que je ne savais pas ce qui allait se passer et qu'ils ne m'ont rien expliqué. Et beaucoup de gens étaient autour et le garde a parlé avec les autres gardes sans m'adresser la parole. J'ai alors dû attendre et je ne savais toujours pas pourquoi j'étais là.* »
(Passager en provenance de l'Angola, homme, interrogé à l'aéroport de Schiphol)

« Je comprends vraiment les [...] gardes-frontières. Pour eux aussi, c'est vraiment difficile de travailler des heures et des heures aux guichets ! Donc il arrive parfois que leur comportement laisse un peu à désirer, qu'ils crient sur des gens comme nous, par exemple. » (Homme, ressortissant turc, conducteur de camion traversant régulièrement la frontière, Kipi)

La somme de ces expériences individuelles peut avoir des effets néfastes sur le plan collectif [19]. Cela peut contribuer à une nette détérioration de la relation entre la police et les fonctionnaires chargés de la gestion des frontières, d'une part, et les membres des communautés minoritaires faisant l'objet de contrôles et de fouilles fréquents ou de vérifications approfondies aux frontières, d'autre part.

19 Nations unies (NU) (2007), paragraphe 57.

Étude de cas

Le rôle des contrôles et des fouilles dans l'enclenchement de troubles publics (Royaume-Uni 2011 et France 2005)

Au lendemain des émeutes survenues dans plusieurs grandes villes du Royaume-Uni en août 2011, la London School of Economics et le journal *The Guardian* ont interrogé 270 personnes sur les raisons de leur participation aux émeutes. L'étude a révélé que la méfiance et l'antipathie à l'égard de la police ont été un facteur important, et que «[l]es plaintes les plus fréquentes avaient trait à l'expérience quotidienne des personnes avec la police, nombre d'entre elles faisant part d'une grande frustration quant à la manière dont les personnes de leurs communautés étaient traitées lors des opérations de contrôle et de fouille ».

Pour de plus amples informations, voir London School of Economics (2011).

Des dynamiques similaires ont été recensées dans d'autres États membres de l'UE. En France, les émeutes de novembre 2005 semblent avoir été déclenchées par un événement impliquant la mort accidentelle de deux jeunes issus de minorités alors qu'ils étaient poursuivis par la police (voir Jobard, 2008, et Body-Gendrot, 2016).

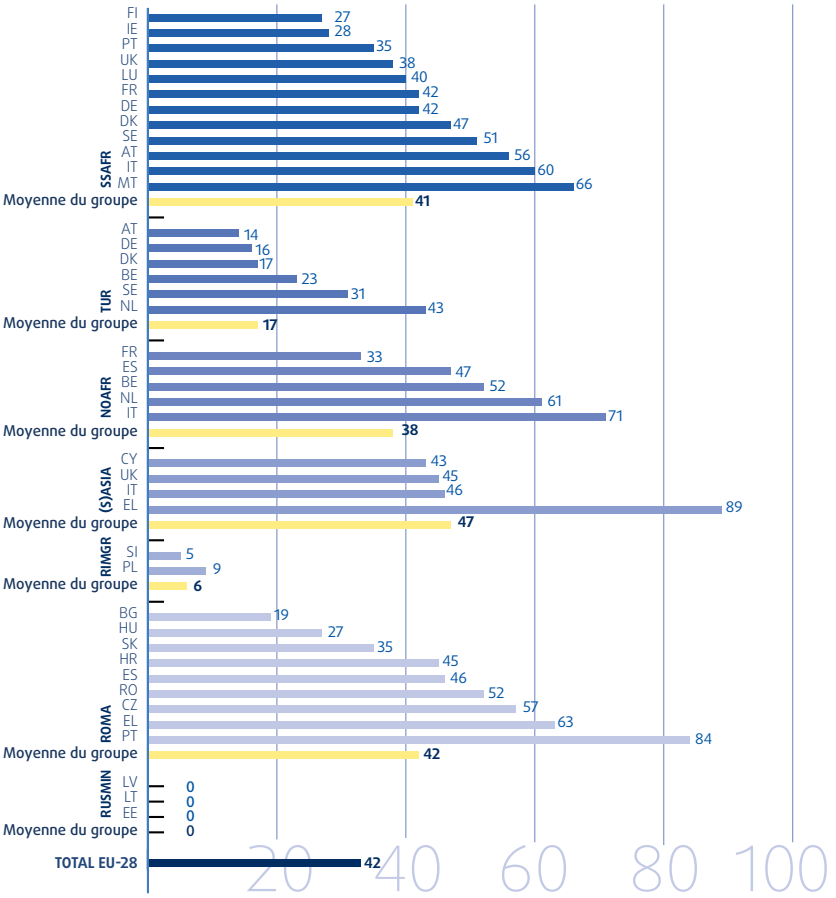
Pour de plus amples informations, voir Hörnqvist (2016).

Dans le même ordre d'idées, le profilage peut donner lieu à une hostilité grandissante dans d'autres interactions entre les individus et la police ou d'autres organes chargés de l'application de la loi. Cette hostilité grandissante augmente les chances que les interactions de routine dégénèrent en agression et en conflit, ce qui pose des problèmes de sécurité pour les fonctionnaires et les membres de la communauté.

Plus généralement, des études récentes montrent que le fait d'être contrôlé, arrêté, condamné ou emprisonné tend à éloigner les personnes des autres services publics, au-delà du système de justice pénale, tels que la santé, l'emploi et les organisations éducatives [20]. Sans remettre en cause les raisons légitimes qui ont conduit à l'arrestation des personnes condamnées, il convient de garder à l'esprit que l'exclusion des groupes déjà marginalisés de la population de ces institutions peut nuire à l'inclusion sociale et à l'intégration des groupes minoritaires.

20 Brayne, S. (2014), p. 367-391.

Figure 3 : Dernier contrôle de police en date perçu comme étant un profilage ethnique par les répondants qui ont été contrôlés au cours des cinq années précédant l'enquête EU-MIDIS II, par État membre et par groupe cible (%) [a,b,c,d]



Remarques : [a] *Parmi les répondants qui ont été contrôlés par la police au cours des cinq années précédant l'enquête (n = 6 787) ; résultats pondérés.*

[b] *Les résultats fondés sur un faible nombre de réponses sont statistiquement moins fiables. Ainsi, les résultats fondés sur 20 à 49 observations non pondérées dans le total d'un groupe,*

ou sur des cellules incluant moins de 20 observations non pondérées, sont notés entre parenthèses. Les résultats fondés sur moins de 20 observations non pondérées dans le total d'un groupe ne sont pas publiés.

[c] *Questions : « Au cours des cinq dernières années en/au [PAYS] (ou depuis que vous vivez en/au [PAYS]), avez-vous déjà été contrôlé, fouillé ou interrogé par la police ? » ; « Pensez-vous que LA DERNIÈRE FOIS que vous avez été contrôlé, ce contrôle était dû à votre origine ethnique ou immigrée ? »*

[d] *Les acronymes des groupes cibles se rapportent aux immigrés de [pays/région] et à leurs descendants : TUR = Turquie, SSAFR = Afrique subsaharienne, NOAFR = Afrique du Nord, SASIA = Asie du Sud, ASIA = Asie, ROMA = minorité rom.*

Source : FRA (2017b).

Plein feu sur les conclusions de l'EU-MIDIS II de la FRA

En 2015 et 2016, la FRA a recueilli des informations auprès de plus de 25 500 personnes appartenant à différentes minorités ethniques et issues de l'immigration dans les 28 États membres de l'UE.

Quelles informations ont été collectées ?

En ce qui concerne le profilage, il a été demandé aux répondants s'ils estimaient avoir été contrôlés par la police parce qu'ils étaient immigrés ou parce qu'ils appartenaient à une minorité ethnique et comment ils ont été traités par la police, notamment s'ils avaient été victimes d'une quelconque expérience d'agression physique de la part de la police. L'enquête ne portait pas sur les interactions avec les agents chargés de la gestion des frontières.

Que montrent les résultats ?

Contrôles et origine ethnique : les résultats montrent que 26 % de tous les répondants EU-MIDIS II ont été contrôlés par la police au cours des cinq années précédant l'enquête. Parmi ceux qui ont été contrôlés au cours des cinq années qui ont précédé l'enquête, 33 % ont déclaré que cela était dû à leur origine ethnique ou à leur condition d'immigré.

Perception de la discrimination : en moyenne, près d'un répondant sur deux originaires d'Asie (47 %), d'Afrique subsaharienne (41 %) et d'Afrique du Nord (38 %) et qui ont été contrôlés pendant cette période ont déclaré l'avoir

été parce qu'ils étaient issus de l'immigration ou parce qu'ils appartenaient à une minorité ethnique. De même, parmi les répondants roms contrôlés, près d'une personne sur deux (42 %) estimait que cela était dû à son origine ethnique. À l'inverse, ce pourcentage est beaucoup plus faible parmi les personnes interrogées d'origine turque (17 %) (voir figure 3).

Respect : les résultats montrent qu'une majorité (59 %) parmi tous les répondants qui ont été contrôlés par la police au cours des cinq années précédant l'enquête ont estimé qu'ils avaient été traités avec respect (25 % « de manière très respectueuse », 34 % « de manière assez respectueuse »). Un sur quatre (24 %) a déclaré que la manière dont la police les avait traités n'était « ni respectueuse, ni irrespectueuse ». Dans l'intervalle, 17 % des personnes interrogées ont déclaré avoir été mal traitées par la police (8 % « de manière assez irrespectueuse » et 9 % « de manière très irrespectueuse »). Les répondants roms et les répondants d'origine nord-africaine contrôlés ont indiqué avoir subi un comportement irrespectueux de la police lors de leur dernier contrôle en date (25 % et 21 %, respectivement), plus souvent que d'autres groupes cibles.

Pour de plus amples informations, voir FRA (2017b).

Plein feu sur l'importance et l'utilité de collecter des données relatives aux contrôles de police

Sur les 28 États membres de l'UE, le Royaume-Uni est actuellement le seul pays où la collecte de données relatives aux contrôles de police comprend systématiquement des informations sur l'appartenance ethnique des personnes contrôlées (voir également les sections 2.2.5 et 2.3.1).

Les données collectées mesurent la fréquence des « contrôles et fouilles » pour différents groupes ethniques en Angleterre et au Pays de Galles. Les catégories ethniques utilisées sont celles qui figurent dans le recensement britannique de 2001. Ce recensement a retenu 16 catégories, qui ont été regroupées en cinq groupes plus larges :

- Blanc : Anglais/Gallois/Écossais/Nord-Irlandais/Britannique ; Irlandais et tout autre Blanc

- Métis/groupes ethniques multiples : Blanc et Noir des Caraïbes ; Blanc et Noir d'Afrique ; Blanc et Asiatique ; toute autre origine métisse/ethnique multiple.
- Asiatique/Britannique d'origine asiatique : Indien, Pakistanais, Bangladais, toute autre origine asiatique.
- Noir/Africain/Caribéen/Noir d'origine britannique : Africain ; Caribéen ; et Noir/Africain/Caribéen de toute autre origine.
- Autres groupes ethniques : Chinois et autres groupes ethniques.

Les données relatives aux contrôles et aux fouilles qui sont collectées comparent le nombre de personnes contrôlées et fouillées dans un groupe ethnique donné au nombre total de personnes de ce groupe ethnique vivant dans la région, à partir desquelles on calcule un taux pour 1 000 personnes.

Pour la période 2016-2017, l'analyse des données recueillies montre que chaque tranche de 1 000 Blancs a fait l'objet de quatre contrôles, contre 29 contrôles pour chaque tranche de 1 000 Noirs. Les données indiquent également que les taux les plus élevés ont été relevés parmi les trois groupes ethniques noirs, à savoir Autres Noirs (70 contrôles pour 1 000 personnes), Noirs des Caraïbes (28 pour 1 000 personnes) et Noirs d'Afrique (19 pour 1 000 personnes).

Sans les preuves fournies par des données ventilées, il est difficile de prouver qu'il existe des différences dans l'action de la police à l'égard de groupes ethniques particuliers et, si tel est le cas, si ces différences peuvent résulter de pratiques de profilage discriminatoires. Des données ventilées sont disponibles dans le domaine public en Angleterre et au Pays de Galles, réparties par force de police. Elles permettent d'épingler les pratiques différentielles entre les forces qui peuvent être considérées comme légitimes ou qui pourraient être utilisées pour identifier une discrimination potentielle dans les pratiques policières. Les données sont également utilisées au niveau des agents de police individuels pour identifier les pratiques discriminatoires dans leur travail.

Pour de plus amples informations, voir la page web de Gov.uk sur les contrôles et les fouilles, le site web de l'Independent Office for Police Conduct et le site web sur les données ouvertes sur le crime et la police du ministère de l'intérieur. Voir aussi Royaume-Uni (2018).

Pour des orientations sur les méthodes de consignation, voir Open Society Justice Initiative (2018b).

Étude de cas

Enquête sur les relations entre la police et la population en France

En 2016, le Défenseur des droits a mené une enquête sur l'accès aux droits. Le Défenseur des droits fait également office de commission nationale d'examen des plaintes en matière de police. L'enquête a porté sur un échantillon représentatif de plus de 5 000 personnes.

La première partie du rapport présente les résultats liés au comportement des services de police. Dans l'ensemble, l'enquête met en évidence des relations satisfaisantes entre la population et les forces de l'ordre. La grande majorité des personnes interrogées dit avoir confiance dans la police (82 %).

En ce qui concerne plus spécifiquement les contrôles d'identité, l'enquête montre que le contrôle d'identité apparaît comme une situation rarement expérimentée : 84 % des personnes interrogées ont déclaré ne jamais avoir été contrôlées dans les cinq dernières années (90 % des femmes et 77 % des hommes). Les personnes contrôlées rapportent généralement peu de comportements en contradiction avec la déontologie des forces de sécurité lors de contrôles plus récents, comme le tutoiement (16 %), la brutalité (8 %) ou les insultes (7 %). Toutefois, 29 % des répondants ont signalé un manque de politesse, et plus de la moitié des répondants (59 %) contrôlés ont indiqué que les raisons du contrôle n'avaient pas été expliquées. D'une manière générale, les contrôles d'identité sont perçus comme plus légitimes lorsque les forces de sécurité prennent le temps d'expliquer les raisons du contrôle.

Les données révèlent également que certains groupes de personnes font état d'expériences plus négatives. Les jeunes hommes de 18 à 24 ans déclarent ainsi sept fois plus de contrôles d'identité fréquents (c'est-à-dire plus de cinq fois au cours des cinq dernières années) que l'ensemble de la population et les hommes perçus comme noirs ou arabes apparaissent entre six et onze fois plus concernés par des contrôles fréquents que le reste de la population masculine. Si l'on combine ces deux critères, 80 % des personnes correspondant au profil de jeune homme de moins de 25 ans perçu comme

noir ou arabe déclarent avoir été contrôlées au moins une fois au cours des cinq dernières années (contre 16 % pour le reste des répondants). Par rapport à l'ensemble de la population, ce groupe a une probabilité 20 fois plus élevée d'être contrôlé.

En outre, les jeunes hommes considérés comme noirs ou arabes ont déclaré une incidence plus élevée de comportements problématiques lors du contrôle d'identité le plus récent, tels que le tutoiement (40 % contre 16 % de l'échantillon total), les insultes (21 % contre 7 % de l'échantillon total) ou la brutalité (20 % contre 8 % de l'échantillon total). Ces expériences négatives et la fréquence des contrôles sont associées à un faible niveau de confiance envers les forces de police. En effet, ce groupe a fait état d'une détérioration dans ses relations avec la police.

Dernier constat : les personnes déclarant des manquements à la déontologie professionnelle lors des contrôles engagent très rarement des démarches pour faire reconnaître cette situation (5 %), principalement parce que ces démarches sont considérées comme inutiles.

Pour de plus amples informations, voir Défenseur des droits (2017).

Lorsque des profils généraux sont appliqués à un groupe minoritaire, ceux-ci, conjointement avec d'autres actions de stigmatisation par la police, peuvent amener ce groupe à développer une perception négative de lui-même. En outre, la communauté au sens large peut développer une perception négative de ce groupe. Le groupe minoritaire peut devenir une « communauté suspecte » associée par le public à la criminalité [21]. Il peut en résulter un préjudice grandissant.

Le groupe minoritaire peut être la cible d'un dispositif policier disproportionné, qui lui-même entraînera logiquement un nombre plus élevé d'arrestations ou de vérifications aux frontières. En conséquence, il est possible d'établir une relation de cause à effet de type « autoréalisatrice » entre une présence policière intensive et des taux d'arrestation plus élevés (voir encadré) [22].

21 Observatoire européen des phénomènes racistes et xénophobes (2006), p. 54.

22 Harcourt, B. (2004), p. 1329-1330 ; House of Commons Home Affairs Committee (2009), paragraphe 16 ; et NU (2007).

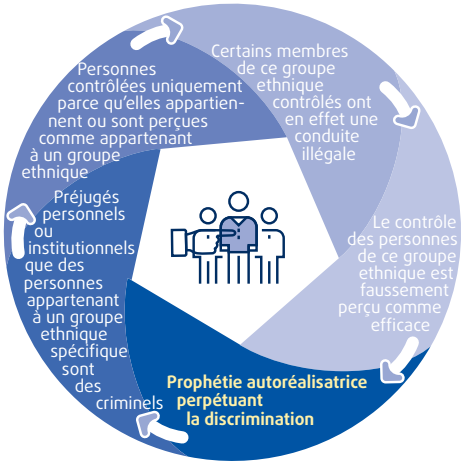
Plein feu sur le risque d'une « prophétie autoréalisatrice »

Lorsque des officiers de police fondent leur profilage non pas sur des motifs objectifs et raisonnables mais sur des préjugés, ils sont susceptibles d'interpréter les informations d'une manière qui confirme leurs propres partis pris. C'est ce que l'on appelle un « préjugé de confirmation ». Ce phénomène se produit lorsque les officiers de police s'attendent à ce qu'un individu agisse illégalement sur la base de préjugés liés à la race, l'origine ethnique, le sexe, l'orientation sexuelle, la religion ou tout autre motif protégé, que ceux-ci soient réels ou supposés. En raison de ce type de parti pris, les agents ayant ces préjugés sont susceptibles de sélectionner davantage de personnes qui correspondent à cette description.

Dans la mesure où il est plus probable que des preuves de la criminalité soient trouvées parmi les personnes qui sont contrôlées que parmi celles qui ne le sont pas, ce profilage basé sur des préjugés renforce les stéréotypes existants d'un officier. Cette fausse « preuve » que la décision de contrôler ces personnes était correcte est appelée « prophétie autoréalisatrice ». Un tel profilage fondé sur des partis pris est discriminatoire, illicite, inefficace et perpétue les stéréotypes.

La figure 4 décrit comment la « prophétie autoréalisatrice » perpétue la criminalisation des individus.

Figure 4 : Le cycle de la prophétie autoréalisatrice



Source : FRA (2018).

1.3.2. L'efficacité du profilage

L'efficacité du recours au profilage sur la base de vastes catégories pour la détection de la criminalité pose également question. Il est difficile de déterminer si le profilage augmente effectivement le taux de réussite des opérations de police.

Certains éléments donnent à penser que la fréquence à laquelle les individus sont contrôlés ne correspond pas nécessairement aux taux d'infraction des différents groupes ethniques ou raciaux (voir encadré). Il convient de noter que, dans la plupart des États membres de l'UE, les données relatives à la justice pénale ne permettent pas d'avoir une vue d'ensemble de l'état d'avancement d'un dossier individuel dans le système de justice pénale. À ce titre, il n'est pas possible de déterminer si une arrestation donne lieu à des poursuites et à des condamnations.

Étude de cas

Un changement de modèle des fouilles engendre un « taux de réussite » plus élevé (1998-2000, États-Unis)

En 1998, 43 % des fouilles effectuées par la douane américaine ont été menées sur des personnes noires et latino-américaines, soit un taux beaucoup plus élevé que leur proportion parmi les voyageurs. Un nombre particulièrement important de fouilles, y compris de fouilles par rayons X et de fouilles corporelles invasives, ont été effectuées sur des femmes latino-américaines et noires suspectées d'être des passeuses de drogue. Cette démarche reposait sur un profil essentiellement basé sur la nationalité et l'origine ethnique. Les taux d'arrestations liés à ces contrôles ont été faibles pour tous les groupes : 5,8 % pour les personnes blanches, 5,9 % pour les personnes noires et 1,4 % pour les personnes latino-américaines. Ce taux était particulièrement faible pour les femmes latino-américaines, qui étaient en fait les moins susceptibles de transporter de la drogue sur ou dans leur corps. En 1999, la douane américaine a changé ses procédures, en supprimant l'origine ethnique des facteurs à prendre en compte lors des contrôles. Au lieu de cela, la douane a choisi de mettre en œuvre des techniques d'observation mettant l'accent sur le comportement, par exemple la nervosité et les incohérences dans les explications des passagers, d'utiliser des informations davantage basées sur les renseignements et d'assurer une surveillance plus étroite des décisions de contrôle et de fouille. En 2000, les disparités raciales dans les fouilles douanières avaient presque disparu. Le nombre de fouilles réalisées a chuté de 75 % et le taux de réussite s'est amélioré, passant d'un peu moins de 5 % à plus de 13 %, et la prévalence des fouilles est devenue quasiment la même pour tous les groupes ethniques.

Pour de plus amples informations, voir Harris (2002), États-Unis (2000).

Inefficacité du profilage illicite (2007-2008, Hongrie)

Les recherches menées en Hongrie ont montré que les Roms étaient la cible d'un nombre disproportionné de contrôles d'identité. Environ 22 % de toutes les personnes contrôlées par la police appartenaient à la communauté rom, alors que la proportion de Roms dans la population était d'environ 6 %. Le nombre disproportionné de contrôles d'identité sur les Roms n'était pas justifié par des preuves d'un comportement illicite : 78 % des contrôles d'identité impliquant des Roms n'ont donné lieu à aucune action de la police, et 19 % étaient liés à une infraction mineure * (contre 18 % pour la

population générale). En outre, les taux d'arrestation pour la communauté rom et la population générale étaient similaires.

Pour plus d'informations, voir Tóth, B.M., et Kádár, A. (2011).

* « Les infractions mineures sont des infractions quasi pénales dont la gravité n'atteint pas le niveau pénal (c'est-à-dire qu'elles ne sont pas réglementées par le code pénal). Les infractions mineures comprennent les infractions passibles d'une incarcération de 60 jours, comme la prostitution ou les menaces physiques, jusqu'aux infractions passibles de mesures moins sévères (par exemple une amende, une confiscation de biens ou une interdiction d'entrer dans certains événements). Les menus larcins ou le petit trafic sont des exemples de ce type d'infraction. » *Voir Kádár, A., Körner, J., Moldova, Z., et Tóth, B. (2008), p. 23.*

Les raisons des contrôles de certaines personnes posent également question. Une étude britannique a révélé qu'«[u]n taux alarmant de 27 % (2 338) des dossiers de contrôle et de fouille examinés [...] ne contenait pas de motifs raisonnables pour procéder à une fouille sur les personnes, même si un nombre important de ces dossiers avaient été approuvés par des supérieurs » [23]. Ceci, note l'étude, suggère que « les forces de police ne se conforment pas totalement aux exigences de l'obligation d'égalité du service public, qui leur impose de veiller scrupuleusement à éliminer la discrimination illicite et promouvoir l'égalité des chances, à encourager de bonnes relations et, à cette fin, de veiller à recueillir, analyser et publier de manière adéquate les données permettant de démontrer qu'elles disposent d'informations suffisantes pour comprendre l'effet de leur travail ».

23 Royaume-Uni, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), p. 6.

2

Le profilage licite : principes et pratique

Le présent chapitre se concentre sur le profilage par les agents de police de première ligne, et notamment sur les opérations de contrôle et de fouille, et par les agents chargés de la gestion des frontières, en particulier dans le cadre du renvoi vers des vérifications de deuxième ligne à la frontière. Il explique les grands principes et pratiques qui peuvent contribuer à réduire le risque de profilage illicite. Ces mesures peuvent être prises tant au niveau de la direction qu'au niveau opérationnel. Il tient compte des différents contextes juridiques et pratiques des opérations de contrôle et de fouille ainsi que des opérations de vérifications aux frontières.

Dans le contexte de la gestion des frontières, le code frontières Schengen [règlement (UE) 2016/399] [24] établit des règles communes régissant les contrôles aux frontières extérieures de l'UE. Cela signifie que certains des principes énoncés dans le présent chapitre — par exemple en ce qui concerne les informations devant être fournies aux ressortissants de pays tiers soumis à une vérification de deuxième ligne — sont prescrits par la loi et lient les États membres. En outre, Frontex joue un rôle important dans la promotion d'un niveau uniformément élevé de contrôles aux frontières. En particulier, le règlement relatif au corps européen de garde-frontières et de garde-côtes de 2016 exige des États membres qu'ils suivent les programmes de base communs mis au point par Frontex pour la formation des gardes-frontières. Publié en 2012, le tronc commun pour la formation (*Common Cure Curriculum*) contient un élément relatif aux droits fondamentaux, qui comprend également le profilage (voir la section 2.2.3 sur la formation ciblée).

24 Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), JO L 77 du 23 mars 2016.

Plein feu sur les motifs d'une vérification de deuxième ligne à la frontière

Le caractère systématique des contrôles aux frontières signifie que chaque voyageur fait l'objet d'une vérification de base de première ligne au cours de laquelle les documents de voyage et tous les autres critères d'entrée sont vérifiés. En outre, certains voyageurs peuvent être sélectionnés pour une vérification supplémentaire de deuxième ligne. Cette décision peut se justifier par diverses raisons : une alerte dans une base de données, un document de voyage suspect, une correspondance avec un profil de risque, ou encore un comportement suspect.

Lors de la vérification de première ligne, le garde-frontière peut s'appuyer sur des informations obtenues en comparant les données figurant dans le document de voyage lisible à la machine (qui comprend des identifiants biométriques) avec les données stockées dans des bases de données nationales, européennes et internationales telles que le système d'information Schengen, le système d'information sur les visas et les bases de données d'Europol et d'Interpol. Dans la pratique, un renvoi vers une vérification de deuxième ligne se produit souvent à la suite d'une alerte dans une des bases de données.

Toutefois, une personne peut également être dirigée vers une vérification de deuxième ligne pour d'autres raisons, par exemple lorsqu'une personne correspond à un profil de risque ou lorsque l'agent a d'autres soupçons sur la personne. Le Catalogue Schengen de l'UE dispose qu'en plus d'effectuer des vérifications aux frontières conformément au code frontières Schengen, l'objectif des vérifications de première ligne devrait être de profiler les passagers et de sélectionner les personnes suspectes pour une vérification approfondie de deuxième ligne *. Les gardes-frontières doivent donc évaluer une combinaison d'autres indicateurs et critères pour déterminer si une personne pourrait tenter une entrée irrégulière, poser un risque pour la sécurité ou, par exemple, être victime de la traite des êtres humains. Qu'ils appliquent ou non un profil de risque spécifique, dans de telles situations, les gardes-frontières utilisent le profilage.

La nécessité d'assurer une circulation fluide des voyageurs signifie que les gardes-frontières ont peu de temps pour apprécier objectivement s'il convient ou non de soumettre une personne à une vérification de deuxième ligne. Les informations fournies par Frontex montrent que les fonctionnaires

des États membres de l'UE ont en moyenne 12 secondes à peine pour décider s'ils doivent diriger un individu vers une vérification supplémentaire **. Ils sont ainsi contraints de prendre rapidement une décision correcte.

* *Conseil de l'Union européenne (2009), Recommandation n° 43.*
** *Agence européenne de garde-frontières et de garde-côtes (Frontex) (2015).*

Les principes et les conseils pratiques de ce chapitre visent à encourager des discussions et la mise en place d'actions concrètes pouvant aider les fonctionnaires et, plus largement, les autorités au sein desquelles ils travaillent, à s'assurer que leurs activités de profilage sont légales. Ces principes sont articulés autour des trois lignes directrices:

- respecter la dignité des personnes ;
- veiller à ce que le profilage repose sur des motifs raisonnables et objectifs ;
- garantir la responsabilité.

Pour chacun d'entre eux, il est fondamental de veiller à ce que les officiers de police et les gardes-frontières respectent la loi lorsqu'ils utilisent le profilage.

2.1. Respect de la dignité des personnes

Points clés

- Garantir une **attitude positive lors des interactions entre la police et les individus** ne garantit pas en soi que le profilage sera non-discriminatoire. Toutefois, une telle attitude positive est susceptible de rendre l'interaction plus fructueuse et de réduire l'impact négatif potentiel des mesures de contrôle et de fouille. Dans le domaine de la gestion des frontières, un comportement professionnel et respectueux constitue une obligation juridique.
- **Un comportement professionnel et respectueux** augmente généralement la satisfaction des personnes quant à leur contact avec les policiers ou gardes-frontières.
- **Expliquer les raisons du contrôle** contribue à renforcer la confiance dans les opérations de police et de gestion des frontières et réduit la perception d'un profilage discriminatoire.
- Le respect et la politesse **ne justifient en aucun cas les vérifications aux frontières ni les mesures de contrôle et de fouille de la police illégales**.

Le respect de la dignité des personnes n'est pas seulement un droit fondamental en soi, mais un principe clé des opérations de police et de gestion des frontières. Dans le cadre des opérations de première ligne, la manière dont les fonctionnaires de la police et de la gestion des frontières s'expriment et interpellent les personnes qu'ils contrôlent, ainsi que les informations qu'ils fournissent, sont essentielles.

Il convient de toujours garder à l'esprit que, quel que soit le degré de politesse et de professionnalisme dont font preuve les agents, le fait de sélectionner des individus en vue d'un contrôle reste une expérience intrusive qui doit toujours être fondée sur des motifs légitimes. La perception d'un profilage discriminatoire est également liée à la fréquence et au nombre d'interactions avec les autorités policières et de gestion des frontières. Il est important dès lors de veiller à ce qu'il y ait toujours des motifs objectifs et raisonnables de contrôler un individu.

Que disent les normes ?

« Les vérifications aux frontières devraient être effectuées de telle manière que la dignité humaine soit pleinement respectée. Le contrôle aux frontières devrait être effectué de façon professionnelle et respectueuse et être proportionné aux objectifs poursuivis. »

Considérant 7 du code frontières Schengen

« Tous les voyageurs ont le droit d'être informés de la nature du contrôle et de recevoir un traitement professionnel, aimable et courtois, conformément au droit international, au droit de l'Union et au droit national applicables. »

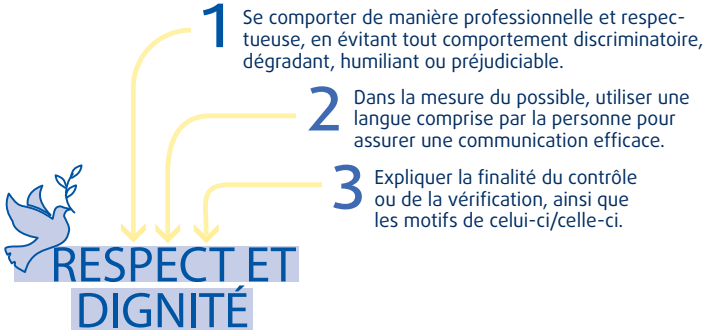
Section 1.2 du manuel pratique à l'intention des gardes-frontières (manuel Schengen)

« Les personnels de police doivent agir avec intégrité et respect envers la population, en tenant tout spécialement compte de la situation des individus faisant partie de groupes particulièrement vulnérables. »

Recommandation nº 44 du code européen d'éthique de la police

Veiller à ce que les agents de police et les gardes-frontières restent courtois et informatifs dans des situations tendues et difficiles n'est pas toujours aisé. Toutefois, les données montrent que l'emploi d'un ton respectueux augmente sensiblement le degré de satisfaction à l'égard de l'interaction [25]. La figure 5 illustre les éléments qui constituent une interaction respectueuse.

Figure 5 : Trois éléments d'une interaction respectueuse



Source : FRA (2018).

25 FRA (2014b).

Certains éléments des vérifications aux frontières sont régis par le code frontières Schengen, tels que l'obligation de procéder à des vérifications de manière professionnelle et respectueuse ou de fournir des informations sur l'objectif de cette vérification et la procédure à suivre (code frontières Schengen, considérant 7, article 7, et article 8, paragraphe 5). L'utilisation d'une langue commune, en revanche, n'est pas une exigence absolue dans le contexte de la gestion des frontières en raison de la nature intrinsèquement variée du trafic frontalier. Néanmoins, le code frontières Schengen exhorte les États membres à encourager les gardes-frontières à apprendre les langues nécessaires à l'exercice de leurs fonctions (article 16, paragraphe 1). Le catalogue Schengen, qui contient une série de recommandations et de bonnes pratiques en matière de contrôle des frontières extérieures, recommande en outre que les gardes-frontières aient la capacité de communiquer dans des langues étrangères liées à leurs tâches quotidiennes. Il s'agit, en tant que bonne pratique, d'avoir une connaissance satisfaisante des langues des pays voisins, ainsi que d'autres langues, en fonction de la nature du trafic frontalier. Idéalement, des fonctionnaires possédant les compétences linguistiques appropriées devraient être inclus dans chaque équipe [26].

Le manque de considération et de respect au cours des contrôles de police peut avoir des effets directs sur l'efficacité des activités de la police (voir la section 1.3.2). Le *Police and Criminal Evidence Act Code of Practice* (code de bonnes pratiques issu de la loi sur la police et les preuves judiciaires) mis au point au Royaume-Uni dispose ce qui suit : « Tous les contrôles et les fouilles doivent être effectués avec courtoisie, considération et respect de la personne concernée. Cela a un impact significatif sur la confiance de la population envers la police. Des efforts raisonnables doivent être consentis afin de réduire autant que possible l'embarras causé à la personne contrôlée » [27].

Certaines composantes importantes du respect de la dignité, telles qu'expliquer les raisons du contrôle et donner aux individus la possibilité d'exprimer leur point de vue, sont des éléments essentiels des procédures de la police et de la gestion des frontières. Les formulaires de contrôle et de fouille peuvent aider à fournir ces informations de manière structurée (voir section 2.3.1).

Dans le contexte de la gestion des frontières, les formulaires types constituent un outil utile pour informer les voyageurs de l'objectif et de la procédure des

26 Conseil de l'Union européenne (2009), recommandations 27 et 41.

27 Royaume-Uni, Home Office (2014a), section 3.1.

vérifications de deuxième ligne. Ils peuvent faciliter la communication avec les voyageurs, à condition qu'ils soient distribués et complétés par des explications orales supplémentaires, le cas échéant. Le code frontières Schengen dispose que les personnes qui font l'objet d'une vérification de deuxième ligne doivent recevoir des informations par écrit, dans une langue qu'ils comprennent ou dont on peut raisonnablement supposer qu'ils la comprennent, sur l'objectif de cette vérification et la procédure à suivre. Ces informations doivent :

- être disponibles dans toutes les langues officielles de l'UE et dans les langues des pays limitrophes du pays concerné ;

- indiquer que le voyageur peut demander le nom ou le numéro de matricule des gardes-frontières effectuant la vérification, ainsi que le nom du point de passage frontalier et la date du franchissement de la frontière.

Les éléments d'une interaction respectueuse associés aux compétences de communication et interpersonnelles sont plus difficiles à définir dans les procédures opérationnelles et peuvent nécessiter des investissements supplémentaires dans la formation. Il peut s'avérer difficile de donner un ton positif à l'interaction en raison :

- des compétences limitées en matière de communication ;

- de l'incapacité à exposer la raison de l'action ; ou

- de l'incapacité à surmonter les préjugés personnels et institutionnels et les stéréotypes négatifs, ainsi que les hostilités nourries par certains groupes au sein de la communauté.

2.2. Motifs raisonnables et objectifs

Points clés

- Les actions liées aux contrôles de police et à la gestion des frontières qui sont fondées sur des indications spécifiques et mises à jour sont plus susceptibles d'être objectives.
- Pour être licites, les opérations de contrôle et de fouille et les renvois vers des vérifications de deuxième ligne lors des contrôles aux frontières doivent être fondés sur des **motifs de suspicion raisonnables et objectifs.** Un « pressentiment » ne peut être considéré comme un motif raisonnable ou objectif pour contrôler et fouiller une personne ou la diriger vers une vérification de deuxième ligne lors des contrôles aux frontières.
- Les caractéristiques protégées telles que la race, l'origine ethnique, le sexe ou la religion peuvent figurer parmi les facteurs pris en compte par les services de police et les gardes-frontières pour exercer leurs pouvoirs, mais elles **ne peuvent être la seule ou principale raison de sélectionner un individu.**
- Le profilage basé uniquement ou principalement sur un ou plusieurs des motifs protégés équivaut à une discrimination directe et est illégal.

L'objectivité est un principe important des activités de la police et de la gestion des frontières. Dans le cadre du profilage, les personnes ne devraient être contrôlées et fouillées ou faire l'objet d'une vérification de deuxième ligne que sur la base de motifs de suspicion raisonnables et objectifs. Le comportement de l'intéressé, des renseignements spécifiques ou des circonstances qui relient une personne ou des personnes à une activité illégale présumée sont des justifications objectives.

Pour garantir l'objectivité du profilage, il convient :

- d'éviter les préjugés, notamment par des orientations claires et une formation ciblée ; et
- d'utiliser efficacement les renseignements et les informations.

2.2.1. Éviter les préjugés

Le Code européen d'éthique de la police fournit des orientations sur la conduite de la police dans des domaines tels que l'action et l'intervention de la police,

la responsabilité et le contrôle de la police [28]. Il souligne le principe général selon lequel : « La police doit mener à bien ses missions d'une manière équitable, en s'inspirant en particulier des principes d'impartialité et de non-discrimination » [29].

Sélectionner les individus en utilisant *comme facteur unique ou déterminant* leur race, leur origine ethnique, leur sexe, leur orientation sexuelle, leur religion, leur handicap ou d'autres motifs prohibés, que ceux-ci soient réels ou supposés, constitue une violation des droits fondamentaux. Cette pratique peut également avoir des conséquences négatives importantes tant pour les autorités publiques que pour les communautés (voir la section 1.3).

Le profilage discriminatoire peut être le reflet à la fois de préjugés individuels et institutionnels. Outre les préjugés personnels, les stéréotypes et les comportements discriminatoires à l'égard des individus peuvent découler de pratiques spécifiques au sein des services de police et des autorités chargées de la gestion des frontières. Rendre les procédures et pratiques institutionnelles plus transparentes peut contribuer à lutter contre la discrimination et la pérennisation des stéréotypes.

L'identification de préjugés profondément ancrés peut s'avérer difficile. Les agents de police et les fonctionnaires chargés de la gestion des frontières peuvent penser qu'ils sélectionnent des personnes sur la base de motifs raisonnables et objectifs (tels que les comportements) alors que ces décisions reflètent en réalité leurs préjugés.

Lors du contrôle des individus, les agents établissent souvent un lien entre la raison de la sélection d'une personne donnée et un « pressentiment » ou une « intuition ». Il est probable que la décision se fonde sur une combinaison d'expertise et d'expériences passées, mais il se peut également qu'elle reflète un préjugé conscient ou inconscient de l'agent. Afin d'éviter tout profilage illicite, les agents doivent examiner si leur décision est justifiée par des informations objectives. Le « pressentiment » n'est pas en soi un motif raisonnable ni objectif pour contrôler et fouiller une personne ou la soumettre à une vérification supplémentaire à la frontière.

28 Conseil de l'Europe, Comité des ministres (2001), Recommandation Rec(2001) 10 du Comité des ministres aux États membres sur le Code européen d'éthique de la police, 19 septembre 2001.

29 Ibid., paragraphe 40.

2.2.2. Des guides et instructions clairs à l'intention des agents

La mise à disposition de guides et instructions pratiques, compréhensibles et prêts à l'emploi revêtent une importance particulière pour aider les agents de police et de gestion des frontières qui se trouvent en première ligne à éviter tout profilage illicite. Ces guides peuvent se présenter sous diverses formes : ils peuvent être annexés à la législation, émis par les autorités de police ou de gestion des frontières elles-mêmes, ou bien directement fournis par les hauts responsables. L'utilisation d'exemples concrets pour montrer ce qu'il convient de faire dans des situations particulières est susceptible d'être plus efficace qu'une explication des règles et des procédures.

Ainsi, les fonctionnaires occupant des postes de direction se doivent d'informer leur personnel que des motifs — réels ou supposés — tels que la race, l'origine ethnique, le sexe, l'orientation sexuelle, la religion, ou d'autres motifs de discrimination prohibés, ne peuvent être déterminants pour engager un contrôle ou une fouille d'un individu dans le cadre d'activités policières ou de contrôles aux frontières. Préciser quand et comment ces caractéristiques peuvent être prises en compte contribue à réduire le risque d'interprétations divergentes, ainsi que les décisions fondées sur des stéréotypes et des préjugés. Ces guides et orientations devraient également couvrir les questions liées au respect de la vie privée et à la protection des données personnelles.

Le tableau 3 présente certains types de guides qui peuvent être utilisés, ainsi que les caractéristiques importantes à prendre en compte.

Tableau 3 : Types et caractéristiques des guides et instructions, et rôle des fonctionnaires occupant des postes décisionnels

Types de guides/ instructions	Caractéristiques des guides/instructions	Rôle des fonctionnaires occupant des postes décisionnels
Ceux-ci peuvent être : • inclus aux procédures standards des activités de la police et des gardes-frontières • des codes de conduite • des orientations spécifiques et régulières données par les fonctionnaires occupant des postes décisionnels	Ceux-ci doivent : • être détaillés et spécifiques, et • couvrir toutes les activités pour lesquelles un profilage basé sur des préjugés peut se produire : — contrôle et fouille — arrestations — contrôles aux frontières — utilisation de la force, etc.	Les fonctionnaires occupant des postes décisionnels doivent: • développer ces guides en concertation avec les acteurs de terrain • mettre les guides à disposition des communautés • encourager le retour d'information des communautés sur ces guides et instructions

Source : FRA (2018).

Étude de cas

Code de bonnes pratiques et l'approche dite « des ambassadeurs » (police néerlandaise)

La police néerlandaise a élaboré un code de bonnes pratiques avec des organisations de la société civile, telles qu'Amnesty International, qui décrit les quatre principes d'un contrôle professionnel :

☑ une sélection légitime et justifiable de personnes ;

☑ la fourniture d'explication quant à la raison du contrôle et de la fouille ;

☑ l'utilisation d'une communication professionnelle ;

☑ des agents amenés à réfléchir à leurs pratiques et à fournir un retour d'information.

Il est difficile de modifier des pratiques qui ne sont pas perçues comme problématiques telles que, par exemple, la mise en place de mesures de

police préventives, qui peuvent donner lieu à un profilage ethnique. La police d'Amsterdam a mis au point une approche ascendante impliquant la présence d'agents de terrain (appelés « ambassadeurs ») au sein des équipes de police, aidés de leurs supérieurs et formateurs. La première étape consiste à sensibiliser l'opinion publique en montrant et en discutant de l'impact des contrôles préventifs sur les individus visés et en présentant un cadre alternatif équitable et efficace. La deuxième étape consiste à faire en sorte que les fonctionnaires adhèrent à cette nouvelle pratique.

Pour de plus amples informations en néerlandais, voir le site web de la police.

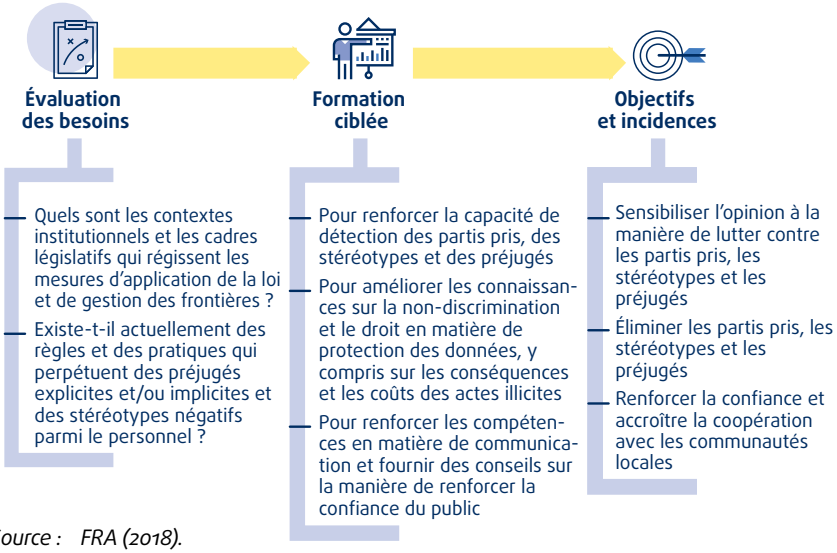
2.2.3. Formation ciblée

La formation des agents de police et des gardes-frontières est un autre outil important pour réduire au minimum le risque de profilage illicite. Il existe différents types de formations, qui peuvent être dispensées à différents stades de la carrière d'un agent, notamment : la formation initiale des recrues, la formation en cours d'emploi et le perfectionnement continu. Quel que soit le type, les modules de formation devraient prendre en considération la culture organisationnelle et proposer des cours intégrant des stratégies de remplacement et de lutte contre les stéréotypes. L'évaluation de l'impact de la formation est également essentielle afin de suivre la manière dont la formation a contribué à l'évolution de la perception des agents et à l'amélioration de leurs pratiques, et afin d'identifier les lacunes dans les domaines où une formation complémentaire pourrait être requise. La figure 6 met en lumière certaines questions à prendre en considération lors de l'élaboration d'une formation ciblée.

Certains types de formations à l'intention des agents de police ou des gardes-frontières sont déjà bien développés dans certains pays, tels que la « formation à la diversité » ou la « formation à la sensibilité ». La formation à la diversité tente de lutter contre les ressentis liés à l'appartenance ethnique, les différences culturelles et les stéréotypes, ainsi que sur la manière dont ils influencent notre vie quotidienne. Toutefois, certains cours de diversité n'abordent pas nécessairement la discrimination. Certaines études font valoir que la formation culturelle et la formation en matière de diversité peuvent en réalité mettre en exergue et renforcer les différences, ce qui a pour effet d'accentuer et non de gommer les stéréotypes [30]. La « formation à la sensibilité culturelle » (par opposition à la « formation générale à la

30 Wrench, J. (2007).

Figure 6 : Le processus et les objectifs d'une formation ciblée



Source : FRA (2018).

diversité ») vise à former les agents de police et les forces de l'ordre à la culture de groupes ethniques spécifiques qu'ils rencontrent fréquemment mais qu'ils ne connaissent pas. Cette formation aborde les choses « à faire et à ne pas faire » et fournit des orientations sur la politesse selon différents points de vue ethniques, religieux ou nationaux. La formation à la sensibilité culturelle est plus efficace lorsqu'elle est mise au point et dispensée avec l'aide et la participation des citoyens des communautés concernées.

Étude de cas

Formation en matière de profilage licite

Formation en matière de profilage à l'intention des agents de police (Italie)

Depuis 2014, l'observatoire italien de la sécurité contre les actes de discrimination *(Osservatorio per la sicurezza contro gli atti discriminatori)* met en œuvre un module de formation sur le profilage ethnique à l'intention des policiers et des cadets. Il met particulièrement l'accent sur les partis-pris présumés qui peuvent influencer le profilage, sur les conséquences en

termes d'efficacité des activités de la police, et sur l'impact négatif des relations avec les communautés. À ce jour, quelque 5 000 personnes ont participé au module de formation. Depuis 2017, un module de formation en ligne a également été fourni dans le cadre de cours de remise à niveau pour la police.

Pour de plus amples informations, voir le site internet de la police nationale italienne.

Instrument relatif aux droits fondamentaux dans la formation des gardes-frontières (UE)

Le tronc commun de formation pour les gardes-frontières européens (*Common Cure Curriculum*) définit les compétences et connaissances de base que chaque garde-frontière européen doit posséder. Il contient des chapitres consacrés à la sociologie et aux droits fondamentaux. Il existe des sections spécifiques consacrées à la non-discrimination (1.5.4) et au profilage ethnique (1.7.10), que les formateurs peuvent utiliser. Le tronc commun souligne les risques potentiels liés aux préjugés, au racisme, à la discrimination raciale, à la xénophobie, à l'islamophobie, à l'homophobie et à d'autres intolérances afférentes présentes lors du profilage. La mise à jour du tronc commun en 2017 a permis l'inclusion de sections sur les nouvelles compétences nécessaires, et en particulier dans le domaine des droits fondamentaux.

En outre, Frontex a mis au point un manuel des formateurs en consultation avec les universités et les organisations internationales [voir Frontex (2013)]. Il fournit aux formateurs des méthodes pour améliorer les connaissances et les compétences des gardes-frontières dans le domaine des droits fondamentaux et de la protection internationale. Le manuel mentionne explicitement le profilage et définit les règles de base permettant d'éviter toute discrimination. La formation est dispensée régulièrement. Toutefois, il n'existe pas de mécanisme permanent permettant d'évaluer la réalisation des objectifs de formation.

Pour de plus amples informations, voir Frontex (2012).

Journées d'étude sur le profilage à l'intention des cadres supérieurs (Belgique)

En 2015, le Centre for Policing and Security (CPS) basé à Gand (Belgique), avec la participation du Centre interfédéral pour l'égalité des chances (Unia), a organisé une journée d'étude consacrée au thème *Profilage ethnique : l'égalité sous pression ?* Cette journée abordait différents aspects de la problématique. Par exemple, les participants ont été amenés à réfléchir sur comment la présence d'agents de police d'origine immigrée pouvait améliorer les relations avec les communautés des minorités ethniques, ou bien sur la fréquence avec laquelle le profilage ethnique est utilisé par les officiers de police, et comment celui-ci a été évalué.

En 2016, Unia a organisé deux journées d'étude à l'intention des hauts responsables de la police du nord de Bruxelles afin de sensibiliser la population au profilage ethnique et de promouvoir la réflexion sur l'identification des pratiques de profilage par les agents de première ligne. Des officiers de police d'Espagne et du Royaume-Uni ont présenté des exemples de bonnes pratiques à un public composé d'agents des forces de l'ordre, de chercheurs et d'ONG. En particulier, ils ont démontré qu'en réduisant le profilage fondé sur l'origine ethnique, les arrestations fructueuses de personnes recherchées ont augmenté. Ils ont fait remarquer que cela a été rendu possible par la tenue de registres corrects sur chaque contrôle, ainsi que par la garantie de la transparence en ce qui concerne les motifs des contrôles. La formation visait à établir une compréhension commune des pratiques de profilage ethnique afin de soutenir le développement futur de la recherche sur les pratiques actuellement mises en œuvre par la police dans ce domaine.

Pour de plus amples informations, voir Belgique (2015 et 2017).

La formation devrait aborder les préjugés et les stéréotypes qui peuvent être ancrés au sein des institutions de police et de gestion des frontières elles-mêmes. Le contexte institutionnel plus large et les politiques internes en place, telles que les mécanismes de plainte existants ou la présence de « code du silence » entre collègues, devraient être examinés avant d'organiser une formation sur la prévention du profilage illicite. Les programmes de formation devraient aborder les préjugés et les stéréotypes intégrés dans les actions de la police, telles que les opérations de contrôle et de fouille, les arrestations, la détention et le recours à la force.

Les officiers de haut rang ou de rang intermédiaire ont un rôle essentiel à jouer dans la réussite de la formation, en tant que participants mais aussi dans l'importance qu'ils attachent à la formation [31]. En tant que bénéficiaires de ces formations, les hauts responsables peuvent apprendre de nouvelles pratiques et de nouvelles compétences qu'ils peuvent transmettre aux agents de première ligne. La culture organisationnelle, largement définie par les équipes de direction, a une incidence considérable sur le comportement quotidien des agents de police et des gardes-frontières, y compris sur la manière dont ils interagissent avec la population.

Les hauts responsables peuvent également veiller à ce que la formation soit perçue de manière positive. Le comportement du personnel occupant des postes de direction, par exemple la manière dont les superviseurs communiquent le but de la formation aux agents ou si les agents pensent qu'ils sont sélectionnés de manière aléatoire ou parce qu'ils sont des « agents problématiques », peut influencer le niveau d'intérêt et d'engagement dans la formation. Encourager les agents à participer activement à des programmes de formation et à être ouverts à des changements de comportement afin d'améliorer leur travail quotidien est de nature à renforcer l'impact de la formation [32].

Une fois la formation achevée, celle-ci devrait être réexaminée et évaluée afin de déterminer son incidence sur la sensibilisation de l'opinion et l'évolution des comportements.

31 Voir Commission européenne (2017b).

32 Miller, J., et Alexandrou, B. (2016).

Plein feu sur les principes directeurs de la formation

Une formation spécialisée est essentielle pour garantir une utilisation licite du profilage. La Commission européenne a élaboré une compilation des grands principes directeurs sur la manière de garantir une formation efficace et de qualité en ce qui concerne les crimes de haine. Les mêmes principes s'appliquent à la formation en matière de profilage licite.

Formation en matière de crimes de haine pour les services de police et les autorités judiciaires pénales : 10 principes directeurs clés

Garantir l'impact et la durabilité :

☑ intégrer la formation dans une approche plus large de lutte contre la discrimination ;

☑ élaborer une méthodologie pour répondre aux besoins de formation.

Définir les objectifs et créer des synergies :

☑ adapter les programmes aux besoins de votre personnel ;

☑ coopérer avec la société civile de manière structurée.

Choisir la bonne méthodologie :

☑ combiner différentes méthodologies ;

☑ former les formateurs.

Transmettre un contenu de qualité :

☑ concevoir un programme de formation avec un contenu de qualité ;

☑ mettre au point des modules de formation axés sur la discrimination.

Suivre et évaluer les résultats :

☑ relier la formation et les processus d'évaluation des performances ;

☑ assurer un suivi et une évaluation réguliers de vos méthodes de formation.

Pour de plus amples informations, voir Commission européenne (2017a).

Une formation ne sera toutefois pas efficace pour contrer les préjugés implicites des agents si elle est dispensée de façon isolée. Ce qu'il faut, c'est un changement de la mentalité institutionnelle. Les autorités doivent donc envisager des interventions multiples pour lutter contre les préjugés personnels et institutionnels (voir l'étude de cas).

Étude de cas

Lutter contre le racisme institutionnel dans la police

Face au bouleversement provoqué par le meurtre raciste de Stephen Lawrence au Royaume-Uni et le rôle joué par le racisme dans la mauvaise gestion de l'enquête policière menée sur cette affaire, le gouvernement britannique a lancé une enquête de grande envergure visant à déterminer « les enseignements à tirer pour les enquêtes et l'exercice de poursuites en cas de crimes à caractère raciste ».

Le rapport de l'enquête, publié en 1999, a mis en évidence le problème du « racisme institutionnel » au sein de la police métropolitaine de Londres, notamment la disparité dans les chiffres relatifs aux contrôles et aux fouilles, qui suscitent une vive inquiétude au sein des communautés concernées. Les recommandations de l'enquête, allant de la sensibilisation au racisme au signalement des incidents, ont été complétées par un appel général à une plus grande ouverture, à la responsabilité et au rétablissement de la confiance par les services de police.

Les réexamens publiés en 2009, dix ans après l'enquête, ont mis en évidence des améliorations dans la manière dont la police interagit avec les communautés ethniques minoritaires et enquête sur des crimes à caractère raciste. Toutefois, ils relèvent que la population noire reste beaucoup plus susceptible d'être contrôlée et fouillée que les Blancs.

Pour de plus amples informations, voir Royaume-Uni, Home Office (1999), Royaume-Uni, Equality and Human Rights Commission (2009) et Royaume-Uni, House of Commons Home Affairs Committee (2009).

2.2.4. Motifs raisonnables de suspicion : le recours aux renseignements et aux informations

Lorsque des officiers de police et des agents chargés de la gestion des frontières sélectionnent une personne pour un contrôle, ils fondent généralement leur décision sur une combinaison d'éléments. Il peut s'agir d'informations plus « objectives », telles que des renseignements, le comportement, les vêtements ou les objets que les personnes transportent, mais aussi de connaissances « subjectives » fondées sur l'expérience.

Tous ces éléments peuvent constituer un « signal » d'une activité illégale. Toutefois, les informations doivent être combinées et utilisées avec prudence. Des éléments tendent à démontrer que les agents peuvent parfois avoir du mal à faire la distinction entre des éléments objectifs et subjectifs dans la pratique, comme dans l'exemple cité dans l'encadré.

Exemple

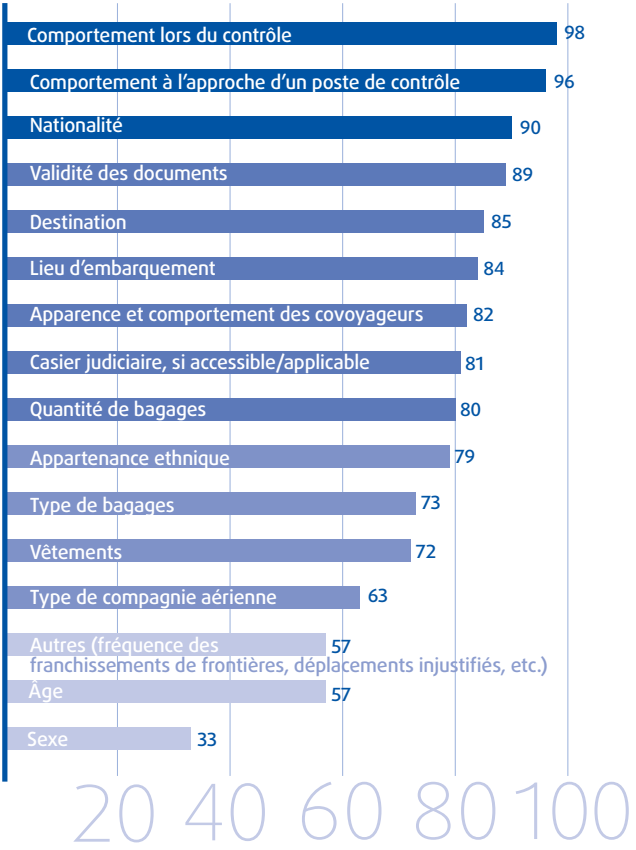
« C'est très subjectif. Il y a d'un côté vos impressions sur les personnes et une affaire, mais il existe également des éléments de preuve de contradictions dans leurs propos, d'incohérences entre ce qu'elles disent et ce que leur regroupant affirme, d'incohérences entre ce qu'elles disent et ce que leurs documents administratifs indiquent, entre ce qu'elles disent et toutes les choses qu'elles peuvent transporter dans leurs sacs. Il y a donc des preuves, mais [ces choses ne peuvent à elles seules] jouer en la défaveur d'une personne. L'agent se doit d'examiner une personne dans sa globalité. »
(Agent de l'immigration dans un grand aéroport britannique)

Pour de plus amples informations, voir FRA (2014a), p. 46.

Plein feu sur l'identification des personnes qui tentent d'entrer clandestinement dans un pays

Les recherches de la FRA menées en 2012 dans plusieurs grands aéroports révèlent que les gardes-frontières prennent en compte un certain nombre de facteurs pour déterminer si une personne tente éventuellement d'entrer dans le pays de manière irrégulière. Il s'agit souvent d'une combinaison de critères

Figure 7 : Indicateurs jugés utiles ou très utiles pour reconnaître efficacement les personnes qui tentent d'entrer dans le pays de manière irrégulière avant que les agents ne s'adressent à eux (%)



Remarque : *Les réponses valables oscillent entre 206 et 216 sur 223. Les répondants qui n'ont pas fourni de réponse à une rubrique donnée ont été exclus du calcul des résultats. Les non-réponses vont de 7 à 17 personnes, selon la rubrique.*

Source : *FRA, Enquête sur les gardes-frontières (2012) (question 17).*

« objectifs » — tels que le comportement de la personne à l'approche du point de contrôle et lors du contrôle, le type et la quantité des bagages, ainsi que la validité des documents de voyage — et de l'expérience personnelle vécue lors de contrôles passés, comme le montre la figure 7.

Les gardes-frontières ont identifié le comportement lors du contrôle ou à l'approche d'un point de contrôle comme étant le facteur le plus utile pour reconnaître les personnes tentant d'entrer dans le pays de manière irrégulière. Toutefois, des facteurs tels que la nationalité et l'origine ethnique, qui pourraient indiquer un profilage discriminatoire, ont également été considérés comme significatifs.

Les vêtements, qui ont également été considérés comme un indicateur utile, illustrent à quel point des informations apparemment « objectives » peuvent être utilisées de manière biaisée dans la pratique. Certains types de vêtements peuvent être associés à des profils de risque spécifiques. Par exemple, les victimes de la traite des êtres humains d'une certaine nationalité peuvent généralement porter des vêtements particuliers. Toutefois, les vêtements peuvent également être le signe d'une appartenance à un groupe ethnique ou religieux spécifique. Même s'il existe suffisamment d'autres raisons pour justifier le renvoi vers une vérification de deuxième ligne, les personnes qui affichent de façon ostentatoire leur origine ethnique ou religieuse, qui ont vécu une expérience passée négative ou qui ne reçoivent pas d'explication adéquate de la part de l'agent, peuvent percevoir le traitement comme étant discriminatoire.

Pour de plus amples informations, voir FRA (2014a). En ce qui concerne les profils des victimes de la traite, voir Frontex (2017).

De bons renseignements sur les modèles de comportements ou des événements peuvent accroître l'objectivité du profilage. Cela pourrait porter sur des activités criminelles ou, dans le cas de la gestion des frontières, sur la migration irrégulière ou la criminalité transfrontalière. Lorsque les mesures de répression et de gestion des frontières reposent sur des renseignements spécifiques et dispensés en temps utile, telles que des informations sur une personne et/ou un contexte particulier, elles sont plus susceptibles d'être objectives et moins susceptibles d'être fondées sur des stéréotypes.

Outre les renseignements et les éléments objectifs, les informations sur les caractéristiques protégées, réelles ou supposées, telles que la race, l'origine ethnique, la nationalité, le sexe ou la religion, peuvent, dans certaines circonstances, être utilisées légitimement en tant qu'élément additionnel dans les évaluations de profilage. Pour que ces informations soient licites, elles doivent être réglementées par la loi, respecter le contenu essentiel des droits et libertés concernés, être proportionnées (c'est-à-dire respecter un équilibre des intérêts) et nécessaires (c'est-à-dire qu'il ne devrait pas y avoir de moyens moins restrictifs disponibles). Il doit exister une raison justifiable, autre que les motifs protégés, pour que les agents traitent une personne différemment des autres personnes du public. La raison doit également se rapporter à la personne en question, comme dans l'exemple présenté dans l'encadré.

Exemple

Des témoins indiquent que le suspect d'un vol portait des chaussures de sport rouges et une casquette noire de base-ball, qu'il mesurait entre 1 m 60 et 1 m 70 et qu'il était perçu comme étant d'origine chinoise. Dans ces circonstances, les autorités de police peuvent légitimement considérer l'origine ethnique comme pertinente pour déterminer si une personne devient un suspect potentiel, étant donné qu'elle est combinée à des renseignements spécifiques.

Plein feu sur les descriptions détaillées des suspects

De bonnes descriptions des suspects peuvent réduire le risque de profilage illicite. Une description d'un suspect consiste à fournir des détails sur une personne, par exemple la couleur de peau, des cheveux, des yeux, la taille et le poids, et les vêtements. Ces informations sont fournies par la victime ou les témoins de l'infraction, ou sur la base d'autres renseignements spécifiques. Une bonne description d'un suspect peut être utilisée par les agents comme base des opérations de contrôle et de fouille, ou pour diriger des personnes vers une vérification de deuxième ligne aux contrôles des frontières.

Toutefois, lorsque les agents de police reçoivent une description trop générale d'un suspect ne précisant que la race, l'origine ethnique ou des caractéristiques similaires, ils ne devraient pas utiliser cette description comme base de leurs opérations. Dans de tels cas, les opérations sont susceptibles de donner lieu à de nombreux contrôles de personnes innocentes présentant les mêmes caractéristiques. Ils devraient alors

chercher à obtenir d'autres renseignements opérationnels spécifiques pour guider leurs enquêtes.

Pour de plus amples informations, voir Commission européenne (2017b).

Des informations qui semblent objectives peuvent en réalité intégrer des préjugés. Des facteurs apparemment objectifs, tels que l'heure, le jour, le lieu, etc., peuvent être utilisés indirectement comme motifs de discrimination prohibés, tels que la race, la nationalité, le sexe, l'orientation sexuelle ou la religion, réels ou supposés, comme le montre l'exemple ci-dessous.

Exemple

Une opération de contrôle et de fouille est menée aux alentours de midi, vendredi, dans la zone X. Toutefois, il s'agit là d'un créneau horaire connu pour être un moment de prière privilégié par les musulmans. Comme la zone X est proche d'une mosquée, des facteurs prétendument objectifs tels que l'heure, la date et le lieu pourraient en fait servir de valeurs de substitution pour des opérations de contrôle et de fouille fondées sur le motif discriminatoire interdit de la religion.

De même, la recherche de certains comportements suspects peut sembler être un moyen objectif de détecter d'éventuels actes répréhensibles. Toutefois, les agents peuvent interpréter le comportement d'une personne de différentes manières, en fonction des autres caractéristiques de la personne concernée. Des données tendent à démontrer que la connaissance et la compréhension professionnelles des renseignements peuvent varier considérablement d'un agent à l'autre et ne correspondent souvent pas aux schémas criminels rencontrés dans la réalité [33].

La fourniture en temps utile de renseignements détaillés à l'intention des agents, par exemple lors des « réunions de briefing de changement d'équipe » à chaque changement d'équipe, devrait réduire le pouvoir discrétionnaire des agents et les aider à cibler plus spécifiquement leurs pouvoirs sur les schémas criminels actuels et sur les problèmes de sécurité recensés. Cela réduit l'influence des préjugés. L'amélioration de la qualité et de l'utilisation des renseignements pour se concentrer sur

33 United Kingdom National Policing Improvement Agency (NPIA) (2012).

des facteurs comportementaux ou des informations spécifiques est plus efficace lorsqu'elle est associée à une surveillance et à un suivi renforcés de la manière dont les agents exercent leurs pouvoirs.

Étude de cas

Garantir l'objectivité du profilage

Séances d'information avant le changement d'équipe (UE)

Le Catalogue Schengen recommande qu'avant chaque changement d'équipe, l'agent en service fournisse des informations sur les indicateurs de risque et les profils de risque. Assurer des chevauchements entre les équipes de travail permet de laisser suffisamment de temps pour les échanges d'informations entre le personnel des équipes sortantes et celui des équipes entrantes, et des briefings adéquats.

Pour de plus amples informations, voir Conseil de l'Union européenne (2009).

Programme de formation SDR (Pays-Bas)

Le programme de formation Search, Detect and React (SDR ou Chercher, Détecter et Réagir) vise à prévenir la criminalité ou les actes terroristes avant qu'ils ne surviennent en renforçant la capacité du personnel de sécurité en matière de profilage comportemental. Cela signifie que l'on écarte désormais les caractéristiques inaltérables telles que la couleur de la peau pour se recentrer sur le comportement des personnes pour justifier les décisions en matière d'intervention de police. Étant donné que les indicateurs de comportement suspect sont spécifiques au contexte, la formation est nuancée en fonction de l'environnement. Elle rejette l'idée qu'il existe une solution unique. Une fois ces types de comportement identifiés, les policiers doivent intervenir de façon adaptée. Dans la plupart des cas, ils s'adresseront uniquement au suspect de façon informelle sans exercer aucun pouvoir de police officiel. Le programme comprend un volet d'enseignement en classe, de formation appliquée et d'exercices pendant le service.

Pour plus d'informations, veuillez consulter le site web de la SDR Academy.

L'outil d'Authorised Professional Practice (APP ou pratique professionnelle autorisée) en matière de contrôle et de fouille (Royaume-Uni)

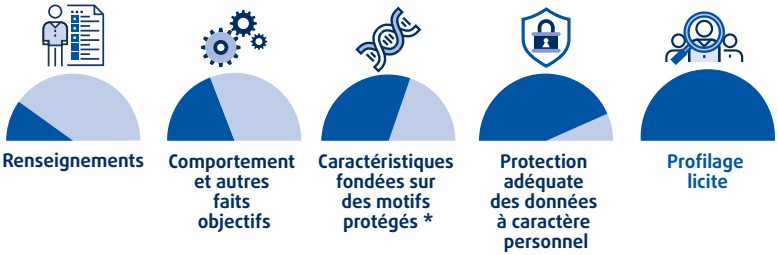
Le College of Policing au Royaume-Uni a élaboré des orientations en matière de pratique professionnelle autorisée couvrant divers aspects du travail de la police. L'APP sur le contrôle et la fouille explique en quoi consistent les contrôles et les fouilles, pourquoi il est important d'utiliser correctement ces pouvoirs, ainsi que les caractéristiques des contrôles et des fouilles licites. Elle explique que la légalité et l'efficacité des contrôles et des fouilles seront assurées en garantissant les critères suivants :

- **équité** : la décision de l'agent de contrôler et de fouiller une personne ne doit reposer que sur des éléments objectifs appropriés. Une personne ne peut jamais être contrôlée uniquement ou principalement sur la base de caractéristiques ou de facteurs protégés tels que des condamnations antérieures ;
- **légalité** : le contrôle et la fouille doivent avoir une base légale appliquée de manière licite ;
- **professionnalisme** : pendant les contrôles et les fouilles, les agents doivent respecter des règles de conduite professionnelles, notamment le code de déontologie, communiquer efficacement avec les personnes et traiter les personnes avec dignité et respect ;
- **transparence** : l'échange avec la personne doit être correctement enregistré. Il convient d'assurer une surveillance et un suivi efficaces des contrôles et fouilles, ainsi qu'un contrôle public.

Pour de plus amples informations, voir Royaume-Uni, College of Policing (2016).

La figure 8 illustre les différents éléments pouvant être utilisés lors d'un profilage licite ; la façon dont ils sont combinés dépendra de la nature de l'affaire concernée.

Figure 8 : Combinaison d'éléments



* *Voir la figure 9 pour la liste des motifs protégés en vertu du droit de l'UE. Le profilage ne devrait jamais se fonder uniquement ou principalement sur des caractéristiques protégées.*

Source : FRA (2018).

La figure 9 montre comment ces éléments peuvent être combinés pour garantir que le profilage ne soit pas discriminatoire.

Figure 9 : Éléments d'un profilage non discriminatoire

Remarques : la liste des motifs protégés varie selon les États membres. Pour un aperçu des motifs de discrimination inclus dans les codes pénaux de chaque État membre, voir FRA (2018d). Voir également le site web d'Equinet, le réseau européen des organismes de promotion de l'égalité, qui énumère les motifs de discrimination couverts par les organismes nationaux de promotion de l'égalité.

Source : FRA (2018).

2.2.5. Formulaires et récépissés de contrôle et fouille menés par les services de police

Les formulaires ou récépissés remplis lors des contrôles et fouilles peuvent aider les agents à déterminer si ceux-ci étaient bien fondés sur des motifs raisonnables, et permettent aux hauts responsables de surveiller les pratiques potentiellement discriminatoires dans les contrôles et fouilles pratiqués par les différents agents. Bien qu'ils soient parfois jugés contraignants, ces formulaires permettent de conserver une trace des contrôles qui, une fois rassemblés, fournissent des données indiquant si les contrôles sont effectués de manière légale [34]. Cela peut contribuer à promouvoir l'ouverture et la responsabilisation. Outre l'utilisation de formulaires papier, les nouvelles technologies, telles que les applications mobiles, peuvent être utilisées pour enregistrer ces informations.

Certains points importants à prendre en compte lors de la conception des formulaires de contrôle et de fouille sont décrits dans l'encadré.

Plein feu sur les ingrédients d'un bon formulaire de contrôle et de fouille

Les formulaires de contrôle et de fouille doivent être bien conçus pour être utiles. Premièrement, remplir les formulaires entraîne une charge de travail supplémentaire pour les agents. S'il n'est pas clairement conçu et raisonnablement court, les agents risquent de ne pas remplir la totalité du formulaire, ou de le remplir de manière sommaire. Deuxièmement, les bons formulaires permettent d'extraire et de rassembler facilement les données afin de faciliter le suivi et l'évaluation des opérations de contrôle et de fouille.

Dans la mesure du possible, les formulaires de contrôle et de fouille doivent :

- utiliser des champs à choix multiple qui sont plus rapides à remplir et plus faciles à traiter sur le plan statistique ;
- présenter une liste exhaustive des options pour chaque rubrique ;
- éviter les rubriques ambiguës ;
- être facilement compréhensibles, tant pour l'agent que pour la personne contrôlée ;
- inclure :

34 Royaume-Uni, Stop Watch (2011).

- les motifs légaux de la fouille. Des explications simples plutôt qu'une liste de règles sont préférables ;
- la date, l'heure et le lieu où la personne ou le véhicule a été fouillé ;
- l'objet de la fouille, par exemple le ou les objets recherchés par les agents ;
- l'issue du contrôle ;
- le nom et le commissariat du (des) agent(s) menant la fouille ;
- les données personnelles de la (des) personne(s) fouillée(s), telles que le nom, l'adresse et la nationalité, peuvent être enregistrées. Toutefois, la personne concernée peut refuser de fournir ces informations.

Pour être efficaces, les formulaires doivent être remplis au moment du contrôle.

Une copie doit être remise à la personne contrôlée ou à la personne responsable du véhicule fouillé. Au Royaume-Uni, les personnes interpellées ont le droit de demander une copie du formulaire dans les trois mois suivant le contrôle. De cette manière, le formulaire fait office de preuve du contrôle tant pour la police que pour les personnes contrôlées.

Pour de plus amples informations, voir Royaume-Uni, West Midlands Police (2012), p. 7, et Royaume-Uni, Home Office (2014a).

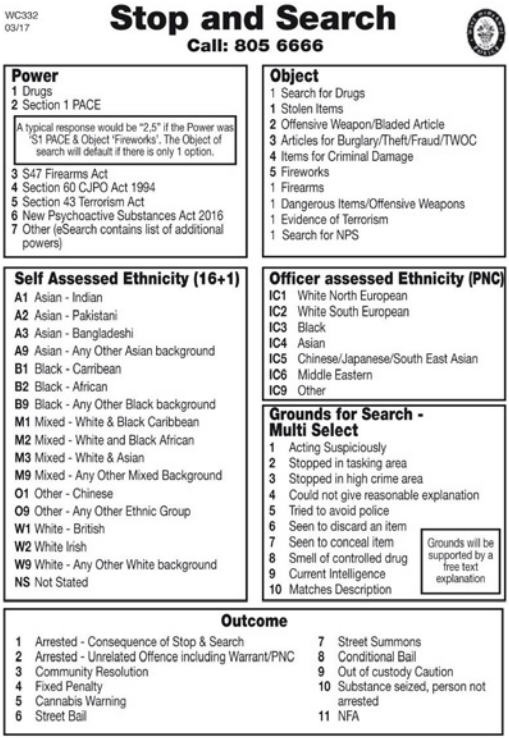
Étude de cas

Formulaire de contrôle et de fouille (Royaume-Uni)

Le formulaire de contrôle et de fouille utilisé par la police des West Midlands au Royaume-Uni est reproduit ci-dessous.

Il montre que la personne interpellée est invitée à s'auto-identifier comme appartenant à l'une des catégories ethniques énumérées, y compris les catégories « autre » ou « non déclarée ». L'agent effectuant le contrôle peut également indiquer sa perception de l'origine ethnique de la personne en cas de désaccord avec celle déclarée.

Le code de bonnes pratiques pour l'exercice des pouvoirs de contrôle et de fouille au Royaume-Uni invite les agents à expliquer aux personnes contrôlées que les informations sur l'appartenance ethnique « sont requises pour obtenir une image fidèle des opérations de contrôle et de fouille et pour contribuer à l'amélioration du contrôle ethnique, à la lutte contre les pratiques discriminatoires et à la promotion d'une utilisation efficace des pouvoirs ».



WC332
03/17

Stop and Search
Call: 805 6666

Power
1 Drugs
2 Section 1 PACE

A typical response would be "2,5" if the Power was 'S1 PACE & Object 'Fireworks'. The Object of search will default if there is only 1 option.

3 S47 Firearms Act
4 Section 60 CJPO Act 1994
5 Section 43 Terrorism Act
6 New Psychoactive Substances Act 2016
7 Other (eSearch contains list of additional powers)

Object
1 Search for Drugs
1 Stolen Items
2 Offensive Weapon/Bladed Article
3 Articles for Burglary/Theft/Fraud/TWOC
4 Items for Criminal Damage
5 Fireworks
1 Firearms
1 Dangerous Items/Offensive Weapons
1 Evidence of Terrorism
1 Search for NPS

Self Assessed Ethnicity (16+1)
A1 Asian - Indian
A2 Asian - Pakistani
A3 Asian - Bangladeshi
A9 Asian - Any Other Asian background
B1 Black - Carribean
B2 Black - African
B9 Black - Any Other Black background
M1 Mixed - White & Black Caribbean
M2 Mixed - White and Black African
M3 Mixed - White & Asian
M9 Mixed - Any Other Mixed Background
O1 Other - Chinese
O9 Other - Any Other Ethnic Group
W1 White - British
W2 White Irish
W9 White - Any Other White background
NS Not Stated

Officer assessed Ethnicity (PNC)
IC1 White North European
IC2 White South European
IC3 Black
IC4 Asian
IC5 Chinese/Japanese/South East Asian
IC6 Middle Eastern
IC9 Other

Grounds for Search - Multi Select
1 Acting Suspiciously
2 Stopped in tasking area
3 Stopped in high crime area
4 Could not give reasonable explanation
5 Tried to avoid police
6 Seen to discard an item
7 Seen to conceal item
8 Smell of controlled drug
9 Current Intelligence
10 Matches Description

Grounds will be supported by a free text explanation

Outcome
1 Arrested - Consequence of Stop & Search
2 Arrested - Unrelated Offence including Warrant/PNC
3 Community Resolution
4 Fixed Penalty
5 Cannabis Warning
6 Street Bail
7 Street Summons
8 Conditional Bail
9 Out of custody Caution
10 Substance seized, person not arrested
11 NFA

Pour de plus amples informations, voir Royaume-Uni, West Midlands Police (2017a) ; et Royaume-Uni, Home Office (2014a), p. 19.

De nombreuses forces de police abandonnent à présent la collecte des données sur les contrôles et les fouilles sur les formulaires et utilisent plutôt des technologies telles que des applications de téléphonie mobile, des systèmes de radiocommunication, des terminaux de données mobiles ou des ordinateurs portables. Ces technologies peuvent accélérer le processus d'enregistrement et réduire la paperasserie,

mais également créer de nouveaux risques, notamment en ce qui concerne l'utilisation algorithmique de données à caractère personnel (voir le chapitre 3).

Étude de cas

Enregistrement en direct des opérations de contrôle et de fouille

« eSearch » (police du comté des West Midlands, Royaume-Uni)

Adopté en avril 2014, ce système est basé sur un appel entre l'agent sur le terrain et un membre du personnel resté au centre de contact (régie). Les détails de l'opération de contrôle et de fouille sont immédiatement enregistrés au centre de contact et intégrés dans une base de données. Ces informations peuvent ensuite être consultées et utilisées pour contrôler l'efficacité des mesures de contrôle et de fouille, à la fois en interne et en externe. eSearch a transformé l'enregistrement des opérations de contrôle et de fouille. Les registres peuvent être consultés bien plus rapidement sur les systèmes de police, ce qui apporte des avantages en matière de renseignement et d'intégration dans les activités opérationnelles de la police.

Pour de plus amples informations, voir Royaume-Uni, West Midlands Police (2014) et Royaume-Uni, West Midlands Police (2016).

Application mobile pour les agents de première ligne (police du comté des West Midlands, Royaume-Uni)

Une nouvelle application mobile lancée en octobre 2017 entend rendre les opérations de contrôle et de fouille plus rapides et plus efficaces. L'application eSearch permet aux agents d'enregistrer les détails des interpellations directement dans l'application au moyen de leurs smartphones, sans qu'il soit nécessaire d'appeler le personnel du centre de contact. Chaque contrôle se voit attribuer un numéro de référence unique et le GPS enregistre automatiquement sa localisation. L'application devrait réduire les appels vers le centre de contact de près de 1 000 appels par mois.

Pour de plus amples informations, voir Royaume-Uni, West Midlands Police (2017b).

Les hauts fonctionnaires de police jouent un rôle important en veillant à ce que les opérations de contrôle et de fouille soient légales. L'exemple ci-dessous montre comment les hauts fonctionnaires peuvent assurer cette surveillance. Ils devraient également veiller à ce que les opérations de contrôle et de fouille ne soient pas utilisées comme une mesure de performance fondée sur le nombre de contrôles effectués.

Étude de cas

Validation des registres de contrôle et de fouille (Royaume-Uni)

Depuis août 2014, chaque registre de contrôle et de fouille au Royaume-Uni doit être validé par le supérieur de l'agent de police ayant procédé à la fouille. Les registres sont approuvés comme étant soit conformes, soit non conformes aux normes en vigueur en la matière. Dans ce dernier cas, l'agent évaluateur doit motiver par écrit sa décision dans le registre de contrôle et de fouille.

Pour de plus amples informations, voir Royaume-Uni, Home Office (2014a).

2.3. Responsabilité

Points clés

- Les fonctionnaires des services de police et de la gestion des frontières sont **responsables** d'assurer un profilage respectueux des lois.
- **La collecte de données fiables, précises et actuelles** sur les activités de profilage est essentielle pour garantir la responsabilité.
- **Des mécanismes de plainte efficaces** peuvent à la fois prévenir les abus de pouvoir et garantir et rétablir la confiance du public dans les opérations des autorités de police et de gestion des frontières.
- **Des réunions de retour d'information avec les citoyens** (afin d'écouter leurs avis, de discuter du profilage et de recueillir un retour d'information sur les opérations) permettent de tirer des enseignements importants et d'améliorer les actions de profilage.

La responsabilité est un principe clé de la gouvernance démocratique. En termes très généraux, il s'agit de fournir des réponses à ceux qui sont en droit de demander des comptes [35]. La responsabilité met non seulement l'accent sur la prise de décision individuelle, mais aussi sur celle de l'institution (la « responsabilité institutionnelle »). En tant que fonctionnaires et organismes publics, les agents de police et de gestion des frontières, ainsi que leurs organisations, doivent rendre compte au public de leurs décisions et actions. Cela inclut l'obligation de veiller à ce que le profilage soit conforme à la loi.

La collecte de données fiables, précises et actuelles est essentielle pour garantir la responsabilité. Dans la mesure où une grande partie des données contiennent des informations personnelles sensibles, elles doivent être traitées conformément aux règles et procédures en matière de protection des données (voir le chapitre 3).

Liste de contrôle de la responsabilité

La liste de contrôle ci-dessous donne un bref aperçu des mesures que les services de police et les autorités chargées de la gestion des frontières peuvent prendre pour veiller au respect de l'obligation de rendre des comptes quant à leurs décisions et actions en matière de profilage. Cette liste peut aider les agents à renforcer leur responsabilisation, mais elle ne doit pas être considérée comme une procédure obligatoire devant être suivie par les agents de police et les agents chargés de la gestion des frontières. En fonction du contexte, certaines recommandations peuvent ne pas s'appliquer aux spécificités de la gestion des frontières.

1. Identifier

- ☑ Constater et **reconnaître** le problème du profilage illicite. Les préjugés et les stéréotypes existent et créent des risques pour les acteurs concernés, y compris les fonctionnaires et les communautés locales.
- ☑ **Collecter et utiliser des données ventilées** : il s'agit d'un outil important pour évaluer l'efficacité et la performance.
- ☑ Participer à des groupes extérieurs organisés par la communauté ou la société civile afin d'obtenir un **retour d'information** sur vos pratiques et de renforcer la confiance dans vos activités.

35 Bovens, M., Schillermans, T., et Goodlin, R. E. (2014), p. 1–11.

2. Collecter des informations

- ☑ Garantir la responsabilité en **tenant des registres** des activités de profilage.
- ☑ Sous réserve des garanties nécessaires, la **vidéosurveillance** et/ou les **caméras piétons** peuvent renforcer la responsabilité et fournir des éléments de preuve à l'appui des actions visant à modifier des modèles de comportement discriminatoires.
- ☑ Créer des **formulaires de contrôle et de fouille** à remplir par les officiers de police après chaque contrôle.

3. Agir et prévenir

- ☑ Mener des **évaluations** afin de déterminer s'il existe des règles et des pratiques qui perpétuent des préjugés explicites ou implicites et des stéréotypes négatifs.
- ☑ Mettre en place des cours spécifiques et/ou des **sessions de formation** axés sur la lutte contre les préjugés et les stéréotypes personnels et institutionnels.
- ☑ **Fournir des informations** aux personnes contrôlées pour renforcer le sentiment d'un contrôle équitable et donner aux personnes des informations suffisantes pour qu'elles décident d'exercer ou non un recours. Pour les renvois vers les vérifications de deuxième ligne aux points de passage frontaliers, la fourniture d'informations est une obligation légale.
- ☑ Faire preuve d'une **tolérance zéro** au sein de l'organisation pour les incidents liés à des préjugés.
- ☑ Établir des **mécanismes internes** de supervision et de contrôle, tels que des groupes internes pour examiner si les contrôles sont effectués sur la base de motifs raisonnables.
- ☑ Veiller à ce que les **indicateurs de performance** soient liés à la prévention des préjugés et des stéréotypes.
- ☑ Établir des **mécanismes de plainte** pour prévenir les abus de pouvoir et garantir la responsabilité.

Source : FRA (2018).

2.3.1. Suivi interne

Le commandement et la direction des services de police et de gestion des frontières jouent un rôle important dans la mise en place d'une éthique respectueuse des droits individuels et du principe de non-discrimination, tant au sein de l'organisation que dans ses relations avec la population. Ils contribuent également à l'instauration d'un climat de responsabilité et de transparence. Une communication ouverte entre les membres du personnel (tant horizontale que verticale) et la définition de normes de comportement claires, telles que des codes de conduite professionnels, sont deux des éléments internes qui devraient être en place pour accroître la responsabilité. Le recrutement et la formation jouent également un rôle important (voir section 2.2.3).

En vertu du droit de l'Union, tout organisme public ou autorité publique est tenu de désigner un **délégué à la protection des données**. Il ou elle conseille les forces de police et de gestion des frontières sur leurs obligations en matière de protection des données, y compris la tenue de registres des activités de traitement des données ou la réalisation d'évaluations d'impact sur la protection des données. Dans le cadre du profilage, le délégué à la protection des données conseillera et veillera, par exemple, à ce que les données à caractère personnel collectées aux fins du profilage ou pendant celui-ci soient traitées et conservées dans le respect de la légalité.

Plein feu sur le rôle des délégués à la protection des données

La **directive « police »** impose aux États membres de désigner un délégué à la protection des données qui est chargé :

- de contrôler le respect de la législation applicable en matière de protection des données à caractère personnel, y compris :
  - la répartition des responsabilités ;
  - la sensibilisation et la formation du personnel ;
  - les audits ;
- de dispenser des conseils en ce qui concerne l'analyse d'impact relative à la protection des données et de vérifier l'exécution de celle-ci ;
- de faire office de point de contact pour l'autorité de contrôle.

Le délégué à la protection des données devrait être associé, de façon entière et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

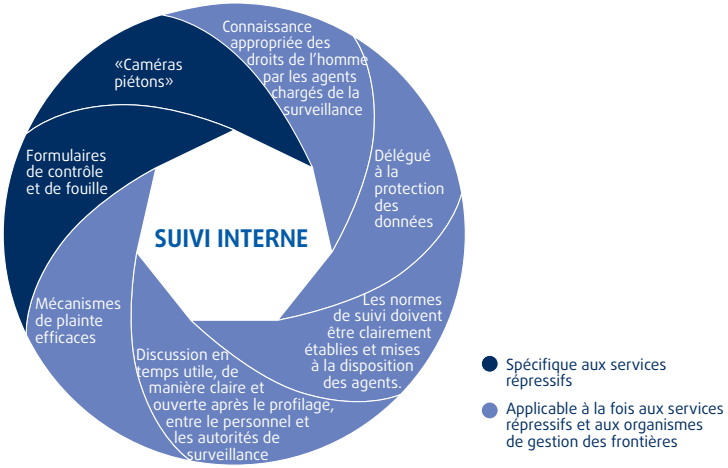
Voir les articles 32 à 34 de la directive « police ».

Au sein des forces de police, le contrôle interne du profilage peut s'effectuer dans le cadre d'un large éventail d'autres mesures visant à tenir des registres des contacts entre les autorités et la population (voir figure 10). Elles impliquent l'utilisation de :

- **formulaires de contrôle et de recherche** qui sont un outil pratique utile pour encourager les agents à effectuer des contrôles fondés et promouvoir l'ouverture et la responsabilité vis-à-vis du public (voir la section 2.2.5) ;

- **caméras piétons :** sous réserve des garanties nécessaires, elles peuvent renforcer la confiance entre les communautés et la police et avoir un effet dissuasif sur l'abus de pouvoir et la discrimination (voir la section 2.3.2).

Figure 10 : Éléments de suivi interne



Source : FRA (2018).

Les activités de contrôle interne des organisations de gestion des frontières peuvent également faire usage de ces mesures. Par exemple, le catalogue de Schengen recommande d'enregistrer le nombre de vérifications de deuxième ligne et les motifs de celles-ci. En outre, les différents contextes des contrôles aux frontières, les infrastructures aux points de passage des frontières et la présence sur place de supérieurs offrent d'autres possibilités de contrôle interne. Par exemple, des équipements technologiques supplémentaires tels que la vidéosurveillance peuvent être disponibles.

Assortis des garanties nécessaires, les enregistrements vidéo peuvent fournir des preuves permettant d'évaluer la manière dont le profilage est effectué, ainsi que des éléments de preuve en cas de plaintes spécifiques. Ils pourraient, par exemple, confirmer que le comportement d'une personne attendant la vérification de première ligne justifiait à lui seul de la diriger vers une vérification de deuxième ligne.

Du fait de la nature publique des points de passage frontaliers et des impératifs de sécurité, les passagers s'attendent à la présence d'équipements de vidéosurveillance, contrairement au contexte des opérations de contrôle et de fouille. Néanmoins, l'utilisation de ces outils doit respecter le droit à la vie privée et les règles applicables en matière de protection des données.

La tenue de registres peut présenter des avantages à court et long terme. L'exemple des formulaires de contrôle et de fouille montre comment :

- à **court terme**, les formulaires de contrôle et de fouille peuvent garantir une responsabilité immédiate. Au Royaume-Uni, toutes les personnes contrôlées reçoivent un procès-verbal du contrôle ou un reçu indiquant où elles peuvent s'en procurer une copie. Il fournit le détail des motifs du contrôle, ainsi que des informations sur comment et où déposer une plainte. Cela permet à la personne de connaître le motif et de le contester si elle l'estime abusif ;

- à **long terme**, l'analyse de ces procès-verbaux permet aux forces de police d'identifier si les pouvoirs de contrôle et de fouille visent de façon disproportionnée certains groupes minoritaires et d'adapter les instructions qu'ils donnent aux policiers en conséquence. Ces procès-verbaux peuvent être rendus publics afin de renforcer la transparence et de promouvoir la confiance du public dans l'utilisation des pouvoirs de contrôle et de fouille.

Tenue de registres : que dit la loi ?

Afin de garantir la licéité du traitement des données, la directive « police » exige que les services de police tiennent un registre de toutes les catégories d'activités de traitement effectuées sous leur responsabilité. En outre, dans les systèmes de traitement automatisé, ils doivent conserver des journaux en vue d'établir l'identité de la personne qui a consulté ou divulgué des données à caractère personnel, le moment où cela s'est produit, le destinataire des données, et la justification du traitement des données (voir la section 3.1.3).

Articles 24 et 25 de la directive « police »

Étude de cas

Utilisation de registres permettant le dépistage de la disproportionnalité des opérations de contrôle et de fouille (Royaume-Uni)

Le Police and Criminal Evidence Act Code of Practice (code de bonnes pratiques issu de la loi sur la police et les preuves judiciaires) élaboré en Angleterre et au Pays de Galles (Royaume-Uni) impose un devoir légal aux forces de police de surveiller le recours aux pouvoirs de contrôle et de fouille pour déceler s'ils sont « exercés sur la base d'images stéréotypées ou de généralisations inappropriées ». Tout recours apparemment disproportionné aux pouvoirs de contrôle par des fonctionnaires ou des groupes de fonctionnaires ou par rapport à des sections spécifiques de la communauté doit être identifié et faire l'objet d'une enquête, et les mesures appropriées doivent être prises pour y remédier. En outre, la police doit prendre des dispositions pour que les registres soient examinés par les représentants de la communauté et expliquer l'utilisation des pouvoirs de contrôle et de fouille au niveau local.

Pour de plus amples informations, voir Royaume-Uni, Home Office (2014a).

Au Royaume-Uni, la police a mis au point plusieurs outils pour accroître la transparence en rendant les données de contrôle et de fouille facilement accessibles. Le site web www.police.uk permet aux utilisateurs de saisir leur code postal pour obtenir des informations détaillées sur le nombre et la nature des contrôles réalisés dans

leur localité. Les informations publiées sont fondées sur les formulaires de contrôle et de fouille complétés. En outre, le tableau de bord des contrôles et fouilles de la Metropolitan Police fournit des données sur tous les contrôles et fouilles réalisés à Londres, y compris sur la proportion de personnes issues de minorités ethniques qui ont été contrôlées par rapport à la population totale. Les utilisateurs peuvent accéder à des données détaillées en ligne de différentes manières, par exemple :

- une carte indiquant, sur une base mensuelle, l'emplacement exact des contrôles et des fouilles effectués dans une zone donnée. L'outil fournit également des informations détaillées sur le contrôle et la fouille (objet, type, issue, si le contrôle et la fouille faisaient partie d'une opération de police), sur la personne (sexe, tranche d'âge, appartenance ethnique autodéclarée, appartenance ethnique déclarée par l'agent), et sur la législation étayant la légalité du contrôle et de la fouille (voir figure 11) ; et

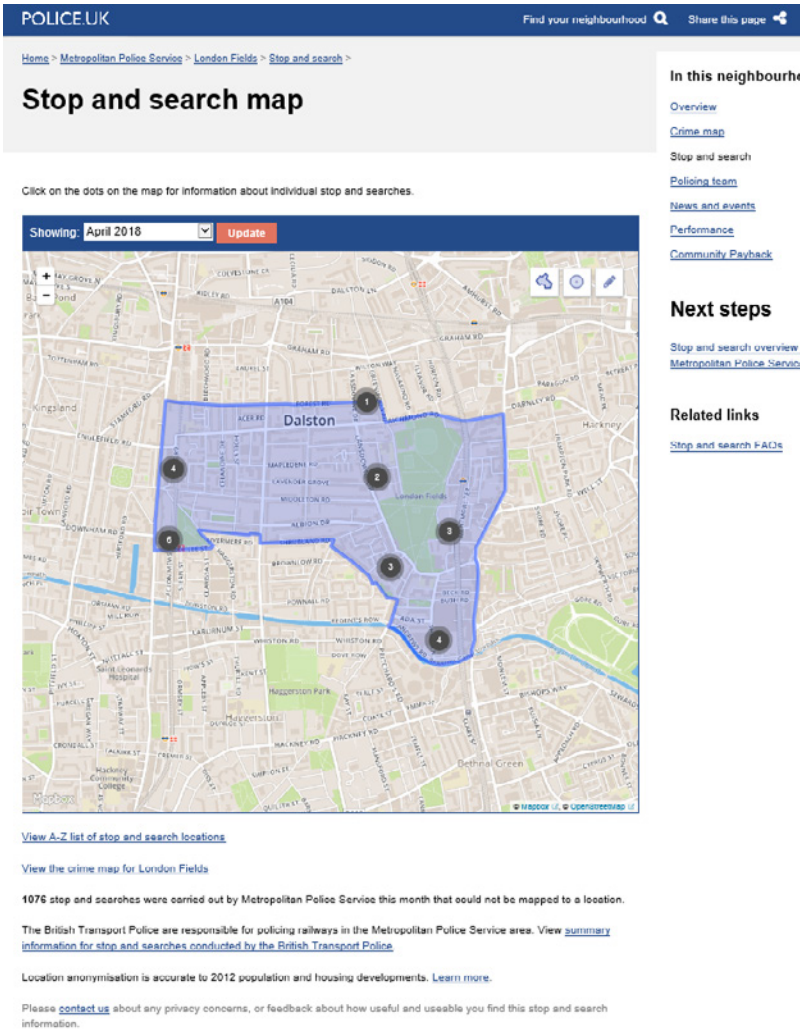
- un aperçu des statistiques et des graphiques présentant les opérations de contrôle et de fouille de la police. Cela permet de regrouper et de télécharger les informations.

Bien que cette pratique favorise la transparence et la confiance, elle pourrait avoir une incidence sur les droits au respect de la vie privée et à la protection des données des personnes concernées. Il est possible que l'identité d'une personne puisse être déduite de la combinaison de données disponibles dans cet outil ou dans d'autres outils en ligne. Ces risques doivent être évalués et, le cas échéant, traités.

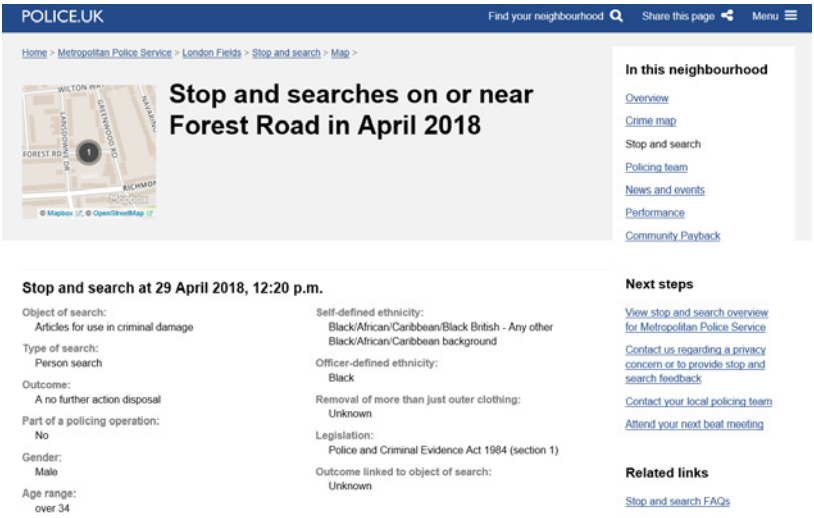
2.3.2. Les caméras piétons

Les forces de police utilisent de plus en plus les caméras piétons. Celles-ci peuvent aider à garantir la responsabilité des agents, à améliorer la qualité des contacts individuels et à modifier les modèles de comportement discriminatoire. Elles peuvent également aider à désamorcer des situations dangereuses. Outre les images recueillies par la police, les membres du public filment de plus en plus des interpellations et d'autres interactions avec la police. Les images peuvent également être utilisées pour examiner les pratiques policières.

Figure 11 : Outil en ligne présentant les détails des opérations de contrôle et de fouille menées à Londres



Source : Royaume-Uni, Home Office, page web sur la carte des contrôles et fouilles.



Source : Royaume-Uni, Home Office, page web sur les fouilles spécifiques.

Étude de cas

L'efficacité des caméras piétons

Une étude menée au Royaume-Uni en 2015 sur l'utilisation de 500 caméras par 814 agents de la Metropolitan Police n'a révélé « aucun impact global sur le nombre ou le type de contrôles et de fouilles réalisés ; aucun effet sur la proportion d'arrestations pour crime violent ; et aucune preuve que les caméras aient changé la manière dont les policiers traitent les victimes ou les suspects ». Les rapports évaluant l'impact d'essais similaires effectués par d'autres forces de police montrent peu ou pas de preuves démontrant que ces essais ont eu un effet positif sur la réduction de la criminalité, sur les plaintes à l'égard des agents, ou sur le recours à la force.

Pour plus d'informations, voir Big Brother Watch (2017).

En France, des caméras piétons ont été déployées dans 300 localités pour une période pilote de deux ans. En juin 2018, un examen réalisé par le

ministère de l'intérieur a mis en évidence les effets et résultats positifs de cette expérience. Le rapport a notamment mis l'accent sur l'effet dissuasif des caméras piétons sur les personnes contrôlées qui se montraient moins enclines à malmener ou insulter la police. Les rapports des municipalités indiquent que l'utilisation de caméras individuelles a permis de réduire l'agressivité et les insultes à l'égard des policiers. Certaines municipalités ont souligné que l'utilisation de caméras piétons par les agents semblait avoir désamorcé des situations conflictuelles qui, sans cela, auraient pu déboucher sur une infraction à l'encontre des policiers. Bien que ces rapports laissent entendre que l'utilité des caméras piétons réside surtout dans l'effet dissuasif du port de ces caméras, certaines séquences ont néanmoins été utilisées comme preuves dans le cadre d'une procédure judiciaire visant à identifier les auteurs d'infractions. Enfin, plusieurs municipalités ont souligné l'utilité pédagogique du dispositif, étant donné que certains agents de police ont été formés aux procédures et techniques d'intervention en visualisant les enregistrements réalisés pendant les interventions. À l'issue du projet pilote, un projet de loi a été présenté au Parlement français en vue d'harmoniser l'utilisation des caméras piétons au sein des forces de police et d'étendre leur utilisation aux pompiers et aux agents pénitentiaires.

Pour plus d'informations, voir France, ministère de l'intérieur (2018).

Un essai d'envergure des caméras piétons sur une durée de 12 mois en 2012-2013 mené à Rialto, aux États-Unis, s'est penché sur la question de savoir si les caméras piétons favorisaient un comportement socialement souhaitable parmi les agents qui les portaient. Les résultats montrent que, par rapport à 2011, au cours de la période d'essai de 12 mois, le recours à la force a chuté de 60 à 25 occurrences et que les plaintes contre la police ont chuté de 28 à 3.

Pour de plus amples informations, voir Farrar, T. (2018).

Toutefois, l'utilisation de caméras piétons par la police soulève d'importants problèmes opérationnels et de droits fondamentaux. Des garanties et des politiques claires relatives à leur utilisation sont nécessaires pour résoudre ces problèmes :

- le **rôle des caméras piétons dans la détection et la dissuasion du profilage illicite** n'est pas clair. Les caméras immortalisent des incidents individuels et ne permettent pas la collecte de données statistiques qui pourraient être utilisées pour déterminer si les opérations de contrôle et de fouille sont discriminatoires.

En lieu et place, les enregistrements peuvent être utilisés pour examiner et discuter des contacts individuels, en contribuant à améliorer leur qualité ;

- l'utilisation de caméras piétons pourrait avoir des **répercussions négatives sur les relations avec les communautés minoritaires**, si elles estiment qu'elles sont spécifiquement ciblées. L'élaboration de garanties et de politiques en concertation avec les communautés locales peut contribuer à promouvoir les caméras piétons en tant qu'outil permettant d'améliorer la responsabilité plutôt que comme un moyen de stigmatiser les groupes minoritaires ;

- l'utilisation de caméras piétons a des **conséquences sur les droits au respect de la vie privée et à la protection des données**, ainsi que sur d'autres droits fondamentaux. Elles pourraient affecter la liberté de réunion pacifique lorsqu'elles sont utilisées pour contrôler les manifestations publiques, par exemple. Il est souvent difficile de déterminer quand les caméras doivent être allumées ou éteintes, et ce qui se passe si un officier oublie ou décide de ne pas allumer la caméra : il y a lieu de fournir des orientations claires sur la question. Les entreprises privées fournissant ce service doivent établir clairement qu'elles ne peuvent en aucun cas traiter les images pour servir leurs propres intérêts. L'utilisation de caméras piétons devrait être réglementée par la loi afin de s'assurer qu'elle est conforme aux droits fondamentaux.

Plein feu sur l'utilisation efficace des caméras piétons

Le respect de trois principes importants peut contribuer à garantir une utilisation efficace des caméras piétons.

- **Authenticité** : les images doivent être clairement liées à l'incident. La date et l'heure (par exemple par horodatage) et la localisation exacte (par exemple par GPS) de l'incident doivent être enregistrées.
- **Fiabilité** : les images doivent être téléchargées dans le système central de manière rigoureuse, sûre et confidentielle. Ces images doivent respecter les principes de protection des données et de respect de la vie privée, et ne doivent donc pas être conservées pendant une période plus longue que celle prévue par la loi.
- **Recevabilité** : pour être utiles dans le cadre des procédures pénales, les images doivent être recevables devant les tribunaux. Cela peut impliquer :

- d'éviter l'enregistrement vidéo continu, ce qui constitue une ingérence inacceptable dans le droit à la vie privée tant des policiers que des personnes filmées ;
- d'informer les personnes qui pourraient être filmées et d'obtenir leur consentement (si nécessaire) ;
- de stocker les images avec un niveau de sécurité adéquat, et de garder une trace de l'accès aux images tant par les officiers de police que par les citoyens.

Pour de plus amples informations, voir Coudert et al. (2015), p. 8.

Les évolutions technologiques futures nécessiteront l'élaboration de nouvelles garanties pour l'utilisation licite des caméras piétons. Par exemple, les caméras capables de reconnaître automatiquement le visage d'une personne en le comparant et en le faisant correspondre à des visages préalablement enregistrés dans une base de données existante posent de nouveaux défis aux droits à la vie privée et à la protection des données.

Étude de cas

Un tableau de bord de l'utilisation des caméras piétons par la police (États-Unis)

En vue de renforcer la transparence et la responsabilité des caméras piétons, la Leadership Conference on Civil and Human Rights & Upturn, aux États-Unis, a mis au point un outil permettant d'évaluer et de structurer les informations pouvant être extraites de séquences filmées par des caméras piétons.

L'outil propose huit critères pour évaluer ces séquences :

1. Les images sont-elles rendues publiques et sont-elles facilement accessibles par le service de police ?

2. Le pouvoir discrétionnaire des agents quant au moment de l'enregistrement est-il clairement indiqué ?

3. Les préoccupations relatives à la protection de la vie privée sont-elles prises en compte ?

4. Les agents doivent-ils passer en revue les séquences avant de rédiger leur premier rapport écrit ?

5. Les séquences non marquées doivent-elles être supprimées dans un délai prédéfini ?

6. Les séquences sont-elles protégées contre toute manipulation ou mauvaise utilisation ?

7. Les séquences sont-elles mises à la disposition des personnes déposant des plaintes ?

8. L'utilisation de technologies biométriques pour identifier les individus dans la séquence est-elle limitée ou non ?

De telles initiatives peuvent contribuer à renforcer la responsabilité en établissant des normes et en encourageant la mise en œuvre de mécanismes permettant d'évaluer si les séquences sont collectées et utilisées de manière appropriée.

Pour de plus amples informations, voir Leadership Conference on Civil and Human Rights & Upturn, site web du tableau de bord.

2.3.3. Mécanismes de plainte

Des mécanismes de plainte efficaces peuvent à la fois prévenir les abus de pouvoir et contribuer à rétablir la confiance du public dans les opérations des autorités de police et de gestion des frontières. Ils coexistent généralement avec les canaux légaux officiels qui permettent aux individus de contester l'action ou la décision d'une autorité publique devant un tribunal indépendant et impartial.

Pour être efficace, il est essentiel que :

- **les individus puissent facilement accéder aux mécanismes de plainte**. Les données montrent invariablement que les gens hésitent à déposer plainte, par

exemple parce que le processus est long ou coûteux, ou parce qu'ils craignent des répercussions négatives. Rendre les mécanismes de plainte facilement accessibles grâce à l'utilisation de plateformes en ligne telles que des sites web ou des applications peut encourager les citoyens à les utiliser. En outre, les organisations peuvent aider les particuliers à introduire des réclamations, soit en déposant des plaintes en leur nom, soit au moyen de mécanismes de recours collectif, comme le prévoit l'article 80, paragraphe 2, du règlement général sur la protection des données ;

- **les plaintes soient traitées de manière transparente**. Cela contribuera à renforcer la confiance dans les mécanismes de plainte ;

- **les organismes de traitement des plaintes soient indépendants** de l'organisation ou de la partie de l'organisation contre laquelle la plainte est dirigée.

Il existe toute une série de mécanismes différents qui viennent traiter des types de plaintes tout aussi différents. La figure 12 donne un aperçu de certains des mécanismes de plainte disponibles dans les États membres de l'UE et au niveau de l'UE.

Les mécanismes en vertu desquels les agents de police se réunissent avec les membres du public pour écouter leurs plaintes, discuter du profilage et obtenir un retour d'information sur leurs activités sont l'occasion de tirer des enseignements importants pour améliorer les processus qui régissent le profilage. Ils sont également un moyen d'associer le public aux activités répressives (voir l'étude de cas).

Étude de cas

Mécanismes de plainte publics dans le secteur répressif

Panels d'examen public (police du comté des West Midlands — Royaume-Uni)

Chacune des huit circonscriptions placées sous la responsabilité de la police des West Midlands (WMP) organise une réunion bimensuelle de son panel d'examen des contrôles et fouilles, qui est présidé par des membres du public. Ces panels évaluent les registres de contrôle et de fouille, veillent à ce que la police respecte la législation en vigueur et donnent aux communautés un moyen de communiquer des plaintes et de soulever des questions préoccupantes. Les ordres du jour et les comptes rendus des réunions

Figure 12 : Aperçu des mécanismes de plainte dans les États membres de l'UE

Source : FRA (2018).

sont publiés en ligne. La WMP a adopté un certain nombre de pratiques supplémentaires impliquant davantage la communauté en vue de rendre les interpellations plus justes et plus ciblées, et de responsabiliser davantage les agents.

Pour de plus amples informations, voir West Midlands Police, page web sur les contrôles et fouilles et Her Majesty's Inspectorate of Constabulary (2016).

Panels de motifs raisonnables (police du comté de Northamptonshire – Royaume-Uni)

La police du Northamptonshire a mis en place des panels sur les motifs raisonnables afin d'associer les citoyens à l'amélioration de leurs opérations de contrôle et de fouille. Ces panels offrent une plateforme de discussion sur l'utilisation des pouvoirs de contrôle et de fouille et sur leurs répercussions pour les communautés. Ils sont présidés par un inspecteur en chef et composés d'un officier de première ligne et de deux membres de la communauté, qui peuvent comprendre des contrevenants ou des anciens contrevenants. Outre le renforcement de la communication entre la police et la population, le panel peut retirer certains de leurs pouvoirs de contrôles aux agents, ou les orienter vers une formation complémentaire afin d'améliorer leurs techniques de contrôle et de fouille.

Pour de plus amples informations, voir la page web sur le panel de la police du Northamptonshire et l'Open Society Justice Initiative (2018a).

Réseau informel de mécanismes de plaintes de la police

Le réseau d'autorités indépendantes chargées des plaintes à l'encontre des forces de police (IPCAN) est un réseau informel d'échange et de coopération entre les structures indépendantes chargées du contrôle externe des forces de sécurité. Il a été créé en 2013 et rassemble les autorités chargées des plaintes d'environ 20 pays, principalement des États membres de l'UE mais pas uniquement. Ces organismes reçoivent et traitent les plaintes à l'encontre des forces de sécurité publiques et, parfois, privées.

Pour de plus amples informations, voir le site web de l'IPCAN.

Dans le cadre de la gestion des frontières, des mécanismes de plainte publics peuvent être mis en œuvre immédiatement ou a posteriori. La possibilité d'accéder à de tels mécanismes accroît la transparence et la responsabilité et encourage le respect mutuel et de bonnes relations entre les gardes-frontières et le public. La possibilité de déposer une plainte a posteriori auprès d'une instance supérieure plutôt que directement (et uniquement) au point de passage frontalier crée un certain niveau de supervision et peut avoir une influence positive sur la volonté des voyageurs de signaler d'éventuels incidents [36].

Étude de cas

Mécanismes de plainte publics pour la gestion des frontières

Mécanisme de plainte interne à l'aéroport de Manchester (Royaume-Uni)

À l'aéroport de Manchester, la plateforme centrale d'attribution constitue un point de contact unique pour tous les passagers qui souhaitent déposer une plainte. Les plaintes peuvent être déposées par courrier électronique, par lettre, par téléphone ou télécopie, ou bien face à face, et elles peuvent être rédigées en anglais ou en gallois. Le document d'orientation sur les forces frontalières du Royaume-Uni décrit les différentes manières de régler les plaintes. Il est généralement possible de régler les fautes mineures telles que l'impolitesse, la brusquerie ou une mauvaise attitude sur place. Les options consistent à clarifier les problèmes avec le client, à expliquer les procédures opérationnelles, à convenir de nouvelles mesures ou à présenter des excuses, le cas échéant. Les plaintes relatives à une faute grave sont généralement confiées au département des normes professionnelles. Les orientations de la force frontalière comprennent un test visant à déceler les signes d'une éventuelle discrimination, ce qui constituerait une faute grave. S'il existe des premiers éléments de preuve attestant que le traitement d'un passager peut s'expliquer par des facteurs autres que la race, l'affaire est généralement soumise à un règlement local.

Pour de plus amples informations, voir FRA (2014a), p. 74.

36 FRA (2014b).

Mécanisme de plainte individuelle de Frontex (UE)

À la suite de l'adoption du nouveau règlement de l'Agence européenne de garde-frontières et de garde-côtes (Frontex) en 2016, Frontex a mis en place un mécanisme de traitement des plaintes individuelles pour surveiller le respect des droits fondamentaux dans les activités de l'Agence. Il s'agit notamment de projets pilotes, d'opérations de retour, d'opérations conjointes, d'interventions rapides aux frontières, de déploiements d'équipes d'appui à la gestion des flux migratoires et d'interventions en matière de retour. Toute personne dont les droits ont été directement affectés par les actions du personnel, y compris le personnel des autorités publiques nationales participant à ces activités de Frontex, peut déposer une plainte auprès de l'officier aux droits fondamentaux de Frontex. Ce dernier décide de sa recevabilité et la transmet au directeur exécutif de Frontex, ainsi qu'aux autorités de l'État membre concerné, si le personnel national est impliqué dans l'atteinte alléguée. La plainte peut être déposée dans n'importe quelle langue, par courrier électronique, courrier postal ou par l'intermédiaire d'un formulaire de plainte en ligne disponible sur le site web de Frontex (http://frontex.europa.eu/complaints/).

Plein feu sur les droits des agents de police

Les officiers de police jouissent des mêmes droits et libertés que les autres personnes et sont protégés par les normes en matière de droits de l'homme dans l'exercice de leurs fonctions. Ils peuvent se prévaloir des droits énoncés dans plusieurs documents internationaux en matière de droits de l'homme tels que la Convention européenne des droits de l'homme (CEDH) ou le Pacte international relatif aux droits civils et politiques (PIDCP). Le Code européen d'éthique de la police précise que « [l]es personnels de police doivent en règle générale bénéficier des mêmes droits civils et politiques que les autres citoyens. Des restrictions à ces droits ne sont possibles que si elles sont nécessaires à l'exercice des fonctions de la police dans une société démocratique, conformément à la loi et à la Convention européenne des droits de l'homme ». L'article 11 de la CEDH prévoit une exception qui fait référence à la liberté de réunion et d'association.

Dans l'exercice de ses fonctions de police, en particulier lorsqu'il exerce ses pouvoirs de police, un officier de police n'agit pas comme une personne privée mais comme un organe de l'État. L'obligation de l'État de respecter

et de protéger les droits de l'homme a donc un effet direct sur les différents moyens dont dispose un policier pour réagir à l'agression. Les droits des officiers de police, qui risquent d'être blessés ou de périr dans l'exercice de leurs fonctions, doivent également être respectés et protégés, par exemple en fournissant un équipement de protection, en planifiant avec soin les opérations de la police ou en prenant des mesures préventives. Des restrictions à ses droits peuvent être nécessaires pour l'exercice des fonctions de police, mais toute limitation de ce type doit refléter le principe de proportionnalité. Étant donné son rôle particulier en tant qu'organe de l'État, la police peut faire face à une plus grande limitation de ses droits qu'un « citoyen ordinaire ». Si l'on prend l'exemple d'une manifestation qui dégénère en violence, un « citoyen ordinaire » peut s'enfuir ou demander de l'aide, alors qu'un officier de police est tenu de protéger les droits de l'homme des autres et de rétablir l'ordre public.

Pour de plus amples informations, voir FRA (2013).

3 Profilage algorithmique

Le profilage algorithmique inclut un ensemble de techniques informatisées qui analysent étape par étape des données afin d'identifier des tendances, des modèles ou des corrélations [37]. Par le profilage, la personne est sélectionnée « sur la base de liens avec d'autres personnes identifiées par l'algorithme, plutôt que sur la base de comportements réels » et « les choix des individus sont structurés en fonction des informations relatives au groupe », plutôt qu'en fonction de leurs propres choix personnels [38].

Le profilage algorithmique peut constituer un moyen efficace pour les services de police et de gestion des frontières d'utiliser les données pour prévenir, détecter et enquêter sur la criminalité. Toutefois, la collecte et le traitement de grands ensembles de données soulèvent un certain nombre de problèmes liés aux droits fondamentaux. Outre l'importance d'éviter les discriminations, le profilage algorithmique introduit de nouveaux risques, en particulier en ce qui concerne les droits à la vie privée et à la protection des données. Cette section se concentre sur ces nouveaux risques. Elle illustre ensuite les défis en matière de droits fondamentaux liés à l'utilisation d'un profilage algorithmique dans des bases de données à grande échelle à des fins de gestion des frontières et de sécurité, et propose des moyens de minimiser ces risques.

37 Pour de plus amples informations sur les algorithmes, voir FRA (2018b), p. 4.

38 Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., et Floridi, L. (2016).

Plein feu sur la police prédictive

Certaines autorités de police utilisent plusieurs logiciels pour prévoir le moment et le lieu où une infraction sera commise. Quelques exemples incluent le système « PredPol » au Royaume-Uni et aux États-Unis, le système de sensibilisation au crime (CAS) aux Pays-Bas, ou « Precobs » en Allemagne et en Suisse. Toutefois, l'efficacité de ces méthodes de police prédictive n'a pas encore été correctement évaluée. Jusqu'à présent, les analyses menées révèlent des conclusions contradictoires, comme le montrent les exemples suivants.

Essais pilotes de la police prédictive dans le Kent (Royaume-Uni) et à Los Angeles (États-Unis)

Au Royaume-Uni et aux États-Unis, la police a mené une expérience visant à comparer — par rapport à une approche plus traditionnelle — un algorithme entièrement automatisé pour recenser les points chauds de la criminalité et ainsi planifier les patrouilles de police en conséquence.

Les résultats ont montré que l'algorithme permettait de mieux anticiper les futurs crimes. Il prévoyait entre 1,4 et 2,2 fois plus de poursuites pénales qu'un analyste de la criminalité utilisant des pratiques traditionnelles en matière de renseignements et de cartographie de la criminalité. En outre, les patrouilles basées sur l'outil prédictif sont plus efficaces, ce qui conduit à une réduction moyenne de 7,4 % du nombre de crimes.

Pour de plus amples informations,voir Mohler, G.O. et al. (2016).

Programme PILOT (Predictive Intelligence Led Operational Targeting ou Ciblage opérationnel prédictif fondé sur les renseignements) au port de Shreveport (États-Unis)

Ce programme fait appel à un modèle prédictif pour recenser de petites zones exposées à un risque important de vols et crimes liés à la propriété, et afin de mettre en œuvre un modèle d'intervention dans ces zones visant à anticiper et prévenir ce type d'infractions. Les résultats de trois districts utilisant le système PILOT ont été comparés à trois districts déployant des opérations de police traditionnelles. Il n'existe aucune preuve statistique

démontrant une réduction plus importante des crimes contre la propriété dans les trois districts examinés utilisant le système PILOT.

Pour de plus amples informations, voir Hunt, P., et al. (2014).

Logiciel Beware (États-Unis)

Le logiciel « Beware » fournit aux agents répondant aux appels d'urgence des notes codées (rouge, jaune et vert) indiquant le niveau de menace de la personne ou du lieu concerné. Le logiciel recherche dans les bases de données, y compris dans les rapports d'arrestation, les registres de propriété, les bases de données commerciales, les recherches approfondies sur le web, les publications sur les réseaux sociaux et dans d'autres bases de données accessibles au public.

Les points forts et les points faibles de ce système n'ont pas été évalués. Toutefois, l'absence de contrôle du processus décisionnel et la nature secrète de l'algorithme, qui est protégé par le secret commercial, ont soulevé des questions quant à la responsabilité. En outre, l'inexactitude potentielle des données collectées et/ou des informations déduites de l'analyse peut limiter l'efficacité globale de l'outil.

Pour de plus amples informations, voir Union américaine pour les libertés civiles (2016).

Étude de cas

Évaluation des incidences et du risque de la police prédictive : l'outil d'évaluation ALGO-CARE

Les effets négatifs potentiels du recours à la police prédictive doivent être pris en considération pour assurer une vue d'ensemble équilibrée et transparente de son incidence sur la société. Une analyse réalisée par un groupe comprenant des universitaires et des agents de police a conclu que, dans la mesure où la police prédictive en est encore au stade expérimental au Royaume-Uni, des évaluations détaillées de son incidence sur la société et sur les individus sont nécessaires. Les recherches font valoir qu'il existe des décisions qui pourraient avoir des conséquences trop importantes sur la

société et les individus pour qu'elles soient influencées par une technologie émergente ; il y a donc lieu de ne pas appliquer une prise de décision algorithmique dans ces situations.

Le groupe a mis au point un cadre de prise de décision appelé ALGO-CARE pour le déploiement d'outils d'évaluation algorithmique dans le contexte policier. Ce cadre vise à orienter les agents de la police lors de l'évaluation des risques potentiels liés à l'utilisation de la police prédictive. Il tente également de traduire les principes essentiels de droit public et des droits de l'homme en des considérations et orientations pratiques pouvant être prises en compte par les organismes du secteur public.

L'outil d'évaluation invite les agents de la police à évaluer l'utilisation de la police prédictive au moyen de huit étapes complémentaires.

- **Consultation :** évaluer l'ampleur de l'intervention humaine.
- **Légalité :** évaluer la justification juridique de l'utilisation de l'algorithme.
- **Granularité :** évaluer si l'algorithme peut présenter un niveau de détail suffisant dans le cas spécifique.
- **Appropriation :** veiller à ce que les forces de police aient la propriété légale et la capacité technique d'accéder, de gérer, de tenir à jour et de corriger régulièrement le code source.
- **Remise en question :** veiller à ce que des mécanismes de supervision et d'audit soient en place.
- **Exactitude :** évaluer si l'algorithme correspond à l'objectif de l'activité de police, s'il est possible de le valider périodiquement et si la probabilité et l'incidence d'une inexactitude représentent un risque acceptable.
- **Responsabilité :** évaluer l'équité, la responsabilité et la transparence de l'algorithme.
- **Explicable :** évaluer l'accessibilité des informations concernant à la fois les règles de prise de décision et l'incidence de chaque facteur sur le résultat final.

Pour de plus amples informations, voir Oswald, M., et al. (2017).

3.1. Le cadre de la protection des données régissant le profilage algorithmique

Le développement et l'utilisation croissante de nouvelles technologies — y compris l'utilisation croissante de grands ensembles de données pour étayer la prise de décision — ont amené l'UE à revoir en profondeur ses règles régissant le traitement des données à caractère personnel en 2016. Les deux nouveaux instruments, à savoir le règlement général sur la protection des données (RGPD) et la directive « police », établissent des principes et des normes importants couvrant toute décision fondée sur des processus décisionnels informatisés, y compris le profilage algorithmique.

Le RGPD et la directive « police » sont entrés en vigueur en mai 2018, ce qui signifie qu'il existe peu d'exemples concrets de mise en œuvre au moment de la rédaction du présent document. La section 1.2.2 décrit les normes juridiques régissant les droits au respect de la vie privée et à la protection des données, et explique certaines des principales différences entre le RGPD et la directive « police » (voir le tableau 2). Le présent chapitre s'appuie sur ces informations pour décrire et expliquer les exigences juridiques relatives au profilage algorithmique introduites par le RGPD et la directive « police ». Parmi celles-ci, citons :

- les données doivent être traitées à des fins précises fondées sur une base juridique spécifique ;
- les personnes doivent être informées du traitement de leurs données à caractère personnel ;
- les données doivent être conservées en toute sécurité ; et
- le traitement illicite des données doit être détecté et évité.

Les agents de police et les gardes-frontières souhaitant des informations complémentaires sur les exigences juridiques décrites dans le présent chapitre devraient se tourner vers les délégués à la protection des données au sein de leurs organisations. En outre, le manuel sur la législation européenne en matière de protection des données élaboré par la FRA, le Contrôleur européen de la protection des données (CEPD) et le Conseil de l'Europe fournit des orientations supplémentaires sur l'application de la directive « police » et du RGPD [39].

Points clés

- Le profilage algorithmique doit être **légitime, nécessaire et proportionné**.
- Les données ne peuvent être traitées sans une **finalité spécifique fondée sur une base juridique**.
- Les individus disposent de droits spécifiques décrits en détail dans les dispositions du RGPD et de la directive « police », notamment :
  - **le droit d'être informé,** y compris de recevoir des informations utiles sur la logique de l'algorithme ;
  - le droit **d'accéder à leurs données à caractère personnel** ;
  - le droit **de déposer une plainte** auprès d'une autorité de contrôle ; et
  - le droit à un **recours juridictionnel effectif.**
- Les données doivent être collectées, traitées et stockées en toute **sécurité**.
- Le traitement illicite des données doit être **évité** et **détecté**.

3.1.1. Les données doivent être traitées dans un but spécifique

Tout traitement de données à caractère personnel doit avoir une base juridique. Cela signifie qu'il ne doit être effectué qu'aux **fins spécifiques** fixées par la loi.

Avant tout traitement, l'agent doit connaître sa finalité. Il pourrait s'agir de déterminer, entre autres :

- Les données traitées permettent-elles de détecter une infraction pénale ?
- Sont-elles traitées en vue de préserver la sécurité publique ?
- Sont-elles traitées pour lutter contre le terrorisme ?

39 FRA, CEPD et Conseil de l'Europe (2018).

Une fois la finalité correctement identifiée, les agents sauront quel cadre juridique, du RGPD ou de la directive « police », s'applique, et donc, quelles sont leurs obligations juridiques qui en découlent. Le tableau 4 indique comment déterminer quel cadre juridique s'applique.

Tableau 4 : Identification du cadre juridique approprié en fonction de la finalité du traitement

1. Dans quel but ces données personnelles sont-elles traitées?	
• **Afin de prévenir, de détecter ou d'enquêter sur des infractions pénales** • **Afin d'exécuter des sanctions pénales** • **Afin de protéger les citoyens ou la société contre des menaces pour la sécurité publique**	• Tout autre but
⬇	⬇
2. La directive « police » s'applique	**2. Le règlement général sur la protection des données s'applique**
⬇	⬇
3. Se référer au droit de l'Union ou au droit national concernant * :	**3. Le traitement ne sera autorisé que s'il est :**
• **les types de données à caractère personnel qui peuvent être traitées, et** • **les finalités spécifiques du traitement des données qui sont autorisées.**	• **consenti** par la personne concernée ; • nécessaire à l'exécution d'un **contrat** ; • nécessaire pour respecter les **obligations légales** ; • nécessaire à la sauvegarde des **intérêts vitaux** d'une personne ; ou • nécessaire à **l'intérêt public**.
⬇	⬇

4. La finalité du profilage est-elle exclue du champ d'application de la directive « police » ?	4. La finalité du profilage est-elle exclue du champ d'application du RGPD ?
Les droits d'être informé, d'accéder à des données à caractère personnel et de demander la modification ou l'effacement des données peuvent être limités (en tout ou en partie) dans les cas suivants : • pour éviter de gêner des **enquêtes**, des recherches ou des procédures officielles ou judiciaires ; • pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ; • pour protéger la sécurité publique ; • pour protéger la sûreté de l'État ; • pour protéger les droits et libertés d'autrui.	Les obligations (transparence, information et notification des violations) et les droits (d'accès, de rectification, d'effacement, d'opposition ou de ne pas faire l'objet d'une procédure de prise de décision automatisée) énoncés dans le RGPD **peuvent être limités** par le droit national ou le droit de l'Union européenne pour garantir : • la sécurité nationale, la défense ou la sécurité publique ; • la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; • d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ; • la protection de l'indépendance de la justice et des procédures judiciaires ; • la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière ; • une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique dans les cas spécifiques ; • la protection de la personne concernée ou des droits et libertés d'autrui ; • l'exécution des demandes de droit civil.

Remarque : ** Les actes nationaux de transposition de la directive « police » sont consultables sur le site web EUR-Lex.*

Source : *FRA (2018).*

3.1.2. Les personnes doivent être informées

L'article 13 de la directive « police» et les articles 13 et 14 du RGPD exigent que les personnes soient informées du traitement de leurs données à caractère personnel. Le tableau 5 décrit quand, comment et quelles informations communiquer à la personne dont les données sont traitées.

Tableau 5 : Obligation de fournir aux personnes les informations du profilage : type de données, moyens de communication et exceptions

Obligation de notification — Liste de contrôle	
À qui ?	Individu dont les données personnelles sont traitées
Comment ?	• langage clair et simple • formulaire facilement accessible • sous la même forme que la demande — *privilégier les moyens électroniques*
Quelles informations communiquer ?	**À propos du traitement :** • nom et coordonnées de votre autorité • coordonnées de votre délégué à la protection des données • les finalités du traitement • la base juridique du traitement • la durée maximale de conservation des données • les types de personnes/organisations qui recevront les données **À propos des droits des personnes :** • le droit **d'introduire une réclamation** auprès d'une autorité de contrôle et les coordonnées de ladite autorité • le droit de demander **l'accès** à ses données à caractère personnel • la **rectification** et/ou **l'effacement** des données à caractère personnel • le droit de demander la **limitation** du traitement
Exceptions	• Pour les demandes excessives (répétitives) ou manifestement infondées • Lorsque l'identité du demandeur ne peut être clairement confirmée • Lorsque la communication d'informations ferait obstruction aux enquêtes • Lorsque la communication d'informations porterait préjudice à la prévention ou aux enquêtes en matière d'infractions pénales • Pour protéger la sécurité publique ou nationale • Pour protéger les droits d'autres personnes

Source : FRA (2018).

Plein feu sur le « droit à l'explication »

En cas de profilage, le RGPD exige que des « informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues » du traitement des données soient fournies à la personne concernée. Ces informations doivent être fournies au moment de la collecte des données (notification) et lorsque la personne demande des informations complémentaires (droit d'accès). Ce droit n'est pas explicitement mentionné dans la directive « police ». Toutefois, le considérant 38 précise que « [le traitement automatisé] devrait être assorti de garanties appropriées, y compris la fourniture d'informations spécifiques à la personne concernée [...] en particulier [...] d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision ».

Ce « droit à l'explication » peut s'avérer difficile à mettre en œuvre dans la pratique. Certaines personnes auront la culture numérique nécessaire pour comprendre le code d'un algorithme, tandis que pour d'autres, des informations simplifiées sur la finalité du traitement et les interconnexions des données utilisées seront suffisantes. L'objectif de compréhension est la clé afin de bien évaluer la pertinence de l'explication fournie. Ainsi, un individu devrait recevoir suffisamment d'informations afin de comprendre l'objet, la raison d'être et les critères qui ont conduit à la décision.

Le droit à une explication n'est pas absolu (voir l'étape 4 du tableau 4). Les États membres peuvent légalement limiter ce droit dans plusieurs cas, tels que: la sécurité nationale, la défense, la sécurité publique, la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière, l'exécution de sanctions pénales, la protection de la personne concernée ou des droits et libertés d'autrui et l'exécution des demandes de droit civil.

La fourniture d'informations raisonnables quant à la finalité et aux conséquences envisagées du traitement est néanmoins une bonne pratique, et est donc souhaitable. La mise au point de moyens simples afin d'expliquer, d'une part, la logique sous-jacente, et d'autre part, les critères utilisés pour parvenir à une décision, renforceront en fin de compte la transparence et la responsabilité.

Pour de plus amples informations, voir RGPD, articles 13 à 15 (droit à l'information et droit d'accès), article 22 (décision individuelle automatisée, y compris le profilage) et article 23 (limitations) ; et la directive « police », article 11 (décision individuelle automatisée, y compris le profilage) et articles 13 à 15 (droit à l'information et droit d'accès).

Voir également Groupe de travail « article 29 » sur la protection des données (2018a).

3.1.3. Conserver les données en toute sécurité : règles en matière de registres, « fichiers journaux » et stockage

Les autorités chargées de la collecte et du traitement de données à caractère personnel à des fins de profilage doivent non seulement traiter des données de manière licite, mais également veiller à ce que les données ne soient pas :

- consultées par des personnes non autorisées ;
- utilisées à d'autres fins que l'objectif initial ; ou
- stockées plus longtemps que nécessaire.

À cette fin, les autorités et les agents de police et de la gestion des frontières doivent veiller à ce que des mesures appropriées soient mises en œuvre pour protéger l'intégrité et la sécurité des données. Ils doivent conserver une trace de tout accès aux données, ainsi que de leur utilisation, en créant et en tenant des registres de toutes les activités ou catégories d'activités de traitement (article 30 du RGPD et article 24 de la directive « police »). Les registres doivent contenir :

- le **nom** et les **coordonnées** des autorités et du délégué à la protection des données ;
- les **finalités** du traitement ;
- les **catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées ;

- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- le **recours au profilage** ;
- une indication de la **base juridique** de l'opération de traitement ;
- dans la mesure du possible, les **délais prévus** pour l'effacement des différentes catégories de données à caractère personnel ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1, du RGPD ou à l'article 29, paragraphe 1, de la directive « police ».

En outre, lorsque le profilage informatisé est mis en œuvre à des fins couvertes par la directive « police » (voir la section 3.2), les autorités doivent conserver les « fichiers journaux » (*logins*) concernant la collecte, la modification, la consultation, la communication, y compris des transferts, l'interconnexion ou l'effacement des données.

Ces registres et « fichiers journaux » aideront les agents à démontrer dans quelle mesure ils/elles ont respecté les obligations découlant du droit à la protection des données à caractère personnel lors d'audits internes et/ou externes. Si, par exemple, une personne dépose une plainte, les autorités de police et de gestion des frontières seront tenues de mettre les registres et les journaux à la disposition des autorités nationales chargées de la protection des données.

Les données à caractère personnel ne devraient pas être conservées plus longtemps que nécessaire pour atteindre l'objectif légitime établi. Le stockage pour des périodes plus longues doit être dûment justifié. Dans de tels cas, les autorités devront veiller à ce que le stockage soit régulièrement réexaminé afin de garantir son intégrité et sa sécurité.

3.1.4. Le traitement illicite doit être détecté et évité

Il est difficile de détecter et de prévenir le traitement illicite de données à caractère personnel. Les compétences spécialisées nécessaires pour comprendre les algorithmes complexes et les bases de données à grande échelle compliquent grandement les contrôles appropriés.

Pour remédier à cette situation, le RGPD et la directive « police » prévoient des garanties destinées à orienter les agents de police et des services de gestion des frontières avant, pendant et après le traitement des données. Il s'agit notamment :

- des analyses d'impact relatives à la protection des données ; et
- de la protection des données dès la conception et par défaut.

Analyses d'impact

Le cadre juridique de l'UE exige que les autorités de police et de gestion des frontières effectuent des analyses d'impact préalablement à tout traitement de données susceptible d'entraîner un risque élevé pour les droits des personnes (article 35 du RGPD et article 27 de la directive « police »). Cela signifie que les analyses d'impact doivent être effectuées non seulement lorsque le résultat du traitement est susceptible de porter atteinte aux normes de protection des données ou de la vie privée, mais aussi dans toute situation pouvant aboutir à une violation *d'un droit fondamental*. Parmi ces droits, nous pouvons citer l'égalité et la non-discrimination, la liberté d'expression et d'information, la liberté de pensée, de conscience et de religion, l'éducation, les soins de santé, ou bien l'asile et la protection en cas d'éloignement, d'expulsion et d'extradition. Les analyses d'impact sont particulièrement importantes lorsque le profilage peut avoir des conséquences juridiques pour les individus. Dans ce cas, le RGPD et la directive « police » exigent que ces analyses d'impact soient réalisées.

Les analyses d'impact doivent être réalisées préalablement au traitement lui-même. Les objectifs de ces analyses d'impact sont toutefois doubles :

- *a priori* : avant le traitement des données, la réalisation d'une analyse d'impact de la qualité des données et/ou de l'algorithme à l'origine du traitement contribuera à détecter les éventuelles violations des droits fondamentaux et, le cas échéant, à y remédier ;
- *a posteriori* : une fois les données traitées, l'agent peut être tenu de démontrer qu'il a agi en toute légalité. L'analyse d'impact peut lui permettre de prouver que toutes les mesures nécessaires pour garantir le respect de la loi ont été mises en œuvre.

Les analyses d'impact aideront également les agents à détecter des préjugés cachés susceptibles d'enfreindre les droits à la protection des données et à la non-discrimination, et d'avoir une incidence sur la qualité du profilage (voir la section 1.3.2).

Plein feu sur les risques liés à l'utilisation d'« algorithmes dynamiques »

Les « algorithmes dynamiques » sont des algorithmes qui sont constamment redéfinis et « améliorés » sur la base de « boucles de rétroaction ». Ces boucles sont créées par les systèmes algorithmiques eux-mêmes et ne peuvent être correctement comprises ni même exprimées dans un langage simple (voir l'article 35 du RGPD et l'article 27 de la directive « police »). Contrairement aux « algorithmes statiques », qui reposent sur des critères préétablis, les « algorithmes dynamiques » génèrent de **nouvelles corrélations** en se redéfinissant constamment.

Des algorithmes dynamiques créent le risque que des programmeurs experts ne connaissent plus, à un moment ou un autre, la logique derrière l'algorithme. Il y a un **risque de reproduire involontairement les préjugés existants** et de perpétuer les inégalités sociales et la stigmatisation de certains groupes. Dans de tels cas, il devient très difficile de garantir la responsabilité et les voies de recours pour les personnes concernées.

Il convient donc **d'éviter ou de réduire** le recours aux « algorithmes dynamiques » afin de minimiser le risque de perdre la trace des critères d'évaluation. Cela permet aux auditeurs internes et externes d'évaluer les algorithmes et de les modifier s'ils sont jugés illégaux. Si l'utilisation d'algorithmes dynamiques est justifiée, les indicateurs de risque sont réexaminés et testés de manière à garantir qu'ils n'entraînent pas de profilage illicite.

Pour de plus amples informations, voir Gandy, O. (2010) et Korff, D. (2015).

Une analyse d'impact peut varier considérablement en fonction du type et du volume de données à caractère personnel traitées, ainsi que du type et de la finalité du traitement. Il peut notamment s'agir de la vérification de la qualité des données, des contrôles techniques des algorithmes de traitement des données et/ou d'un examen complet des objectifs du traitement, etc. La figure 13 définit les critères minimaux à évaluer.

Le Groupe de travail « article 29 » sur la protection des données (désormais remplacé par le Comité européen de la protection des données), qui réunit les autorités nationales de protection des données dans les États membres de l'UE, a élaboré des lignes directrices fournissant de plus amples informations sur les analyses d'impact relatives à la protection des données. Les lignes directrices comprennent une cartographie détaillée des critères à utiliser lors de la réalisation des analyses d'impact [40].

Intégration de la légalité « dès la conception » et « par défaut »

Indépendamment de la question de savoir si une analyse d'impact a détecté la possibilité d'une violation des droits fondamentaux, des mesures peuvent être mises en œuvre afin d'éviter tout risque d'illégalité. Il s'agit de la « protection des données dès la conception » et de la « protection des données par défaut » (article 25 du règlement général sur la protection des données et article 20 de la directive « police »).

La protection des données dès la conception vise à garantir qu'aussi bien *avant* que *pendant* le traitement des données, des mesures techniques et organisationnelles sont mises en œuvre pour garantir les principes de protection des données. Par exemple, dans la mesure du possible, les données à caractère personnel pourraient être « pseudonymisées ». La pseudonymisation est une mesure par laquelle les données à caractère personnel ne peuvent être liées à une personne sans informations supplémentaires, qui sont conservées séparément. La « clé » qui permet de réidentifier les personnes concernées doit être conservée séparément et en lieu sûr [41]. Contrairement aux données anonymisées, les données pseudonymisées sont toujours des données à caractère personnel et doivent donc respecter les règles et les principes de la protection des données.

La protection des données par défaut garantit que « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées » [42]. Cela s'applique à :

- la quantité de données à caractère personnel collectées et stockées ;
- les types de traitement qui peuvent impliquer des données à caractère personnel ;

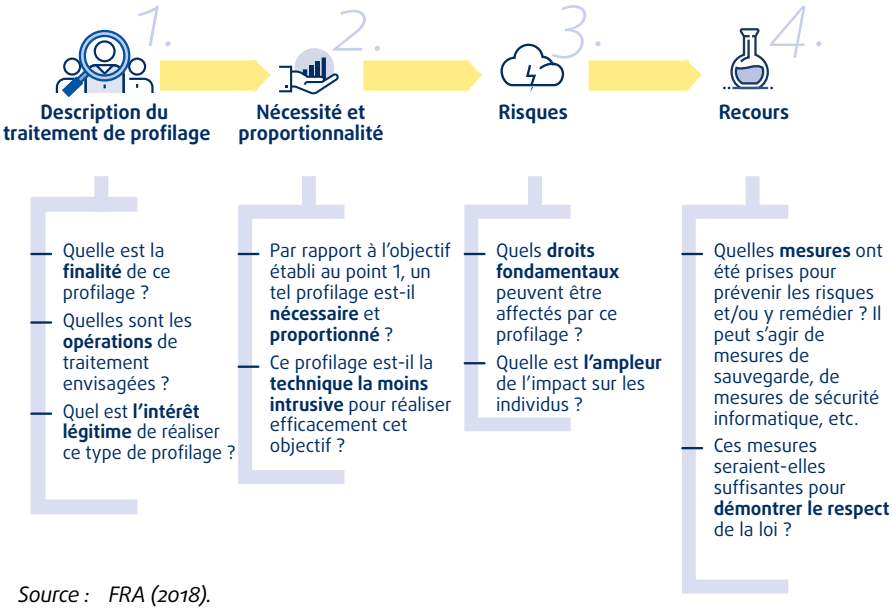
40 Groupe de travail « article 29 » (2017a).

41 FRA, CEPD et Conseil de l'Europe (2018), p. 83.

42 Règlement général sur la protection des données (RGPD), article 25.

- la durée de conservation maximale ;
- le nombre de personnes autorisées à accéder à ces données à caractère personnel.

Figure 13 : Exigences minimales applicables aux analyses d'impact



Source : FRA (2018).

Plein feu sur la responsabilité

L'objectif principal de la protection des données dès la conception et de la protection des données par défaut est de soutenir les autorités de police et les autorités et agents chargés de la gestion des frontières à concevoir des programmes de profilage algorithmique qui respectent les exigences en matière de droits fondamentaux, en particulier les principes de **légalité, de transparence et de sécurité**.

Toutefois, ces mesures peuvent également démontrer comment les autorités respectent l'obligation juridique de **responsabilité**. Les autorités chargées du traitement des données sont également tenues de mettre en œuvre des « mesures techniques et organisationnelles appropriées » pour démontrer

leur conformité avec le droit de l'Union. Par exemple, si une personne dépose une plainte, les autorités judiciaires et les autorités nationales de protection des données peuvent demander aux autorités de démontrer chacun de ces éléments :

- la légitimité, la nécessité et la proportionnalité du profilage informatisé ;
- la licéité de la finalité ;
- les informations fournies aux personnes ;
- l'intégrité et la sécurité des données ;
- les mesures de qualité et les contrôles effectués avant et pendant les opérations de profilage.

3.2. Bases de données à grande échelle pour la gestion des frontières et la sécurité

L'UE a mis au point plusieurs systèmes informatiques ou mécanismes à grande échelle pour la collecte et le traitement des données, qui peuvent être utilisés pour la gestion des frontières et des migrations et, dans une certaine mesure, à des fins répressives. Ils servent d'exemples illustrant certains des défis communs liés à l'utilisation du profilage algorithmique, ainsi que des garanties éventuelles.

Le tableau 6 présente brièvement ces systèmes informatiques et mécanismes de l'UE. L'annexe donne un aperçu détaillé des systèmes informatiques à grande échelle existants et prévus dans l'UE à partir de mars 2018.

Les systèmes informatiques à grande échelle de l'UE sont utilisés dans un certain nombre de processus liés à la migration, notamment le processus d'évaluation des risques préalable à l'arrivée, la procédure d'asile, la procédure de demande de visa, lors des vérifications aux frontières, lors de la délivrance de titres de séjour, lors de l'arrestation des migrants en situation irrégulière, pendant les procédures de retour et pour la délivrance d'interdictions d'entrée. Les systèmes informatiques mis en place par l'UE, y compris ceux créés initialement pour l'asile et la gestion des migrations, sont également de plus en plus utilisés dans le contexte de la sécurité intérieure, par exemple pour les contrôles de police et dans la lutte contre la grande criminalité et le terrorisme.

Tableau 6 : Instruments de l'UE sélectionnés impliquant le traitement de grandes quantités de données pour la gestion des frontières et l'application de la loi

Base de données	Acronyme	Objectif principal
Système d'information Schengen	*SIS II*	Introduire et traiter des signalements concernant des personnes recherchées ou portées disparues aux fins de préserver la sécurité, introduire et traiter des signalements concernant des ressortissants de pays tiers aux fins de non-admission ou d'interdiction de séjour, ainsi qu'introduire et traiter des signalements concernant des ressortissants de pays tiers faisant l'objet d'une décision de retour.
Système d'information sur les visas	*VIS*	Faciliter l'échange de données entre les États membres Schengen sur les demandes de visa.
Système européen de comparaison des empreintes digitales	*Eurodac*	Déterminer l'État membre responsable de l'examen d'une demande de protection internationale et contribuer au contrôle de l'immigration irrégulière et des mouvements secondaires.
Système d'entrée/sortie	*EES*	Calculer et surveiller la durée du séjour autorisé des ressortissants de pays tiers et identifier les personnes ayant dépassé la durée de séjour autorisée.
Dossier passager	*PNR*	Collecter, traiter et échanger les données relatives aux passagers de vols extra-UE en provenance de pays tiers (« vols extra-UE ») *. Utilisé à proprement parler à des fins répressives uniquement.
Information préalable sur les passagers	*API*	Collecter et traiter les données relatives aux passagers des vols en provenance de pays tiers (« vols extra-UE ») à des fins de gestion des frontières et répressives.
Système européen d'information et d'autorisation concernant les voyages	*ETIAS*	Évaluer si un ressortissant d'un pays tiers exempté de visa pose un risque en matière de sécurité, d'immigration irrégulière ou de santé publique.

Système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers	*ECRIS-TCN*	Partager des informations sur les condamnations antérieures de ressortissants de pays tiers.

Remarque : ** En outre, l'article 2 de la directive (UE) 2016/681 donne aux États membres la possibilité de traiter les données provenant des vols intra-UE.*

Source : *FRA (2018).*

La plupart des systèmes mis en place par la législation de l'UE se concentrent sur l'identification d'une personne spécifique en mettant en correspondance des données alphanumériques ou biométriques (actuellement, les empreintes digitales) avec des informations déjà présentes dans le système. À quelques exceptions notables près (voir « Plein feu sur le profilage algorithmique dans les instruments de l'UE »), ils ne contiennent pas eux-mêmes d'algorithme qui permettrait d'associer une personne à un profil. Ils peuvent néanmoins être utilisés pour produire des statistiques anonymisées, y compris sur des caractéristiques qui sont considérées comme des motifs protégés, comme le sexe ou l'âge (voir section 1.2.1).

Ces statistiques pourraient être utilisées pour établir des profils de risque appliqués dans les futures décisions en matière de gestion des frontières ou les futures décisions répressives. Dans le contexte du cadre général pour l'interopérabilité des systèmes d'information de l'UE, l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) sera chargée de la gestion du répertoire central des rapports et statistiques. Ce répertoire s'appuiera sur les données des bases de données existantes de l'UE (système d'entrée/de sortie, ETIAS, système d'information Schengen et système d'information sur les visas) afin de produire des statistiques et des rapports analytiques pour les organes de l'UE et des États membres [43].

43 Commission européenne (2017), proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (frontières et visas) et modifiant la décision 2004/512/CE du Conseil, le règlement (CE) nº 767/2008, la décision 2008/633/JAI du Conseil, le règlement (UE) 2016/399 et le règlement (UE) 2017/2226, COM(2017) 793 final, Strasbourg, 12 décembre 2017 ; Commission européenne (2017), proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (coopération policière et judiciaire, asile et migration), COM(2017) 794 final, Bruxelles, 12 décembre 2017.

Plein feu sur le profilage algorithmique dans les instruments de l'UE

Certains instruments de l'UE prévoient l'utilisation de statistiques extraites de leurs données pour générer des profils de risque. En plus de permettre la détection de suspects « connus », ils contiennent une fonction de profilage algorithmique qui identifie des personnes « inconnues » susceptibles d'intéresser les autorités répressives et de gestion des frontières.

Le système européen d'information et d'autorisation concernant les voyages (ETIAS) [44], adopté en septembre 2018, évalue si les ressortissants de pays tiers exemptés de l'obligation de visa présentent un risque en matière d'immigration irrégulière, de sécurité ou de santé publique avant d'accorder l'autorisation de voyage. Les informations fournies par les voyageurs au cours de la procédure de demande sont comparées automatiquement avec les bases de données pertinentes de l'UE et internationales, ainsi qu'à un ensemble d'indicateurs de risque (ci-après les « règles d'examen ») contenus dans le système ETIAS lui-même. Un algorithme développé par Frontex compare le profil individuel du voyageur (sur la base d'indicateurs tels que l'âge, le sexe, la nationalité, le lieu de résidence, le niveau d'instruction et la profession) avec ces indicateurs de risque afin de déterminer si la demande doit faire l'objet d'un examen manuel.

Les données des dossiers passagers (données PNR) sont recueillies par les transporteurs aériens à partir des informations fournies par les passagers dans les systèmes de réservation de vols, telles que les dates de voyage et l'itinéraire, les coordonnées du passager et le moyen de paiement utilisé, les informations relatives aux bagages et les autres « remarques générales » telles que les préférences alimentaires. Il n'existe pas de base de données centrale de l'UE recueillant ces données, mais la directive PNR de l'UE [45] exige que les transporteurs aériens transmettent les données aux unités d'information passagers (UIP) nationales, qui analysent ensuite les informations aux fins de la lutte contre le terrorisme et les formes graves de criminalité. Outre la détection de la circulation transfrontalière des

44 Commission européenne (2018), règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226, COM(2016) 731 final, Bruxelles, 16 novembre 2016, article 33, paragraphe 5.

45 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, JO L 119, article 6, paragraphe 4.

personnes connues, ces données peuvent être utilisées pour identifier des menaces inconnues à ce jour en traitant les données des passagers au regard d'indicateurs de risques spécifiques (« critères préétablis »). Ces critères sont fixés par les UIP et actualisés sur la base de nouvelles données et de nouveaux modèles disponibles dans le système.

3.2.1. Réduire au minimum les risques en matière de droits fondamentaux liés au traitement des données dans les bases de données à grande échelle

Des données complètes sur les voyageurs, comme la nationalité, le sexe et l'âge, seront utilisées pour le profilage, y compris le profilage algorithmique, à une échelle qui n'était pas possible dans le passé. Même si ces données sont anonymisées, leur traitement n'est pas sans risque. Les partis pris conscients ou inconscients dans la sélection des indicateurs de risque, dans la conception des algorithmes ou dans l'interprétation des résultats pourraient mener à des actions opérationnelles pouvant aboutir à la discrimination de certaines catégories de personnes [46].

La présente section examine certains de ces risques et propose des pistes pour les réduire. Elle s'appuie sur les douze orientations pratiques de la FRA liées aux droits fondamentaux concernant le traitement des données PNR à des fins d'application de la loi (voir l'étude de cas). Bien que formulées dans le contexte spécifique du traitement des données PNR, certaines de ces orientations sont d'application plus générale et peuvent être considérées comme des garanties atténuant les risques découlant du profilage algorithmique.

Étude de cas

Orientations opérationnelles de la FRA pour la mise en place de systèmes PNR nationaux

En 2014, en l'absence de législation au niveau de l'UE en matière de PNR, la Commission européenne a invité la FRA à fournir des orientations pratiques concernant le traitement des données PNR à des fins d'application de la

46 Pour plus d'informations, voir FRA (2017e) et FRA (2018a).

loi, pour les États membres prévoyant d'instaurer leurs propres systèmes nationaux de PNR. Les orientations se sont concentrées sur les droits au respect de la vie privée (article 7 de la Charte), sur la protection des données à caractère personnel (article 8 de la Charte) et sur la non-discrimination (article 21 de la Charte). Certaines des mesures de sauvegarde proposées ont ensuite été introduites dans la directive PNR de l'UE.

Les douze orientations pratiques en matière de droits fondamentaux concernant le traitement des données PNR à des fins d'application de la loi sont les suivantes :

- utiliser les données PNR uniquement pour lutter contre le terrorisme et les formes graves de criminalité transnationale ;
- limiter l'accès à la base de données PNR à une unité spécialisée ;
- ne pas demander un accès direct aux bases de données des compagnies aériennes ;
- supprimer les données PNR sensibles ;
- mettre en place des garanties strictes en matière de sécurité et de traçabilité contre les abus ;
- réduire la probabilité de signaler les faux positifs ;
- être transparent vis-à-vis des passagers ;
- permettre aux personnes d'accéder à leurs données PNR et de les rectifier ;
- ne pas permettre l'identification des personnes concernées ou la conservation des données plus longtemps que nécessaire ;
- transférer les données extraites des données PNR uniquement aux autorités publiques nationales compétentes ;
- ne transférer les données extraites des données PNR vers des pays tiers que dans des conditions strictes ;
- réaliser une évaluation objective et transparente du système PNR.

Pour de plus amples informations, voir FRA (2014c).

Le traitement des données qui révèlent des caractéristiques protégées devrait être nécessaire et proportionné

La nature du profilage algorithmique signifie que l'utilisation de caractéristiques personnelles liées à des motifs protégés comporte un risque particulièrement élevé de discrimination [47]. Dans le contexte de l'UE, la législation ETIAS et la législation PNR interdisent de baser les indicateurs de risque sur des critères qui comportent un risque élevé de discrimination, notamment la race, l'origine ethnique ou les convictions religieuses. Toutefois, même en l'absence de telles données, d'autres types de données peuvent être étroitement liés à ces caractéristiques, en agissant effectivement comme valeurs de substitution pour de telles caractéristiques protégées. Par exemple, la catégorie « remarques générales » des PNR, qui pourrait contenir les préférences alimentaires des voyageurs, pourrait révéler certaines croyances religieuses.

Une combinaison spécifique de données utilisées par l'algorithme peut également désavantager une catégorie de personnes. Elle peut, par exemple, désavantager les personnes en raison de leur origine ethnique ou sociale ou de leur appartenance à une minorité nationale, qui sont des caractéristiques protégées en vertu de l'article 21 de la Charte. Par exemple, dans le système ETIAS, si un profil de risque concernant le risque de migration irrégulière est basé sur la combinaison d'une certaine nationalité et d'un certain groupe professionnel, il peut conduire à cibler un groupe ethnique ou une nationalité qui, dans un pays donné, travaille habituellement dans un secteur économique particulier, comme la construction ou l'agriculture [48].

- Le traitement des données qui révèlent des caractéristiques protégées par l'article 21 de la Charte devrait être limité à ce qui est strictement nécessaire et proportionné et ne devrait jamais entraîner de discrimination. Avant tout traitement, l'autorité compétente devrait évaluer les données afin de déterminer les caractéristiques protégées et d'éliminer toutes les données dont le traitement ne serait pas licite. En tant que bonne pratique, il y a lieu de compléter cela par un programme de mise en concordance et d'élimination avec un glossaire régulièrement mis à jour des « termes sensibles ».

47 Contrôleur européen de la protection des données (2018).

48 Voir également FRA (2017a).

Les critères de profilage devraient être spécifiques et ciblés

Un autre risque découle de l'utilisation de **critères généraux de profilage**. Les instruments existants de l'UE laissent une marge d'appréciation importante pour le développement d'algorithmes de profilage. Pour évaluer le risque de migration irrégulière, ETIAS envisage d'utiliser des statistiques européennes et nationales sur le taux de dépassement de la durée de séjour autorisée et les refus d'entrée. En ce qui concerne les risques pour la sécurité, toutefois, il ne fait généralement référence qu'aux informations concernant des indicateurs de sécurité et des menaces spécifiques. La directive PNR fournit des indications générales sur la conception des algorithmes, mais ne précise pas les critères à utiliser pour identifier les personnes potentiellement impliquées dans une infraction terroriste ou un crime grave, ni le poids à attribuer à un critère spécifique.

Des critères trop généraux conduisent à un nombre important de « faux positifs », ce qui signifie que des personnes se voient attribuer à tort un certain profil de risque. Certains de ces « faux positifs » pourraient également être de nature discriminatoire. Par exemple, une définition large du critère de « condamnation pénale antérieure » signifie que les personnes LGBT seraient tenues de faire état de leurs antécédents judiciaires liés à un comportement sexuel érigé en infraction pénale dans certains pays tiers.

- Les critères d'évaluation doivent être prédéfinis, ciblés, spécifiques, proportionnés et fondés sur des faits. Les critères d'évaluation doivent être testés sur des échantillons anonymisés. Ils devraient faire l'objet d'examens réguliers par un auditeur interne afin de déterminer s'ils sont toujours justifiés par leurs objectifs spécifiques.

- Avant de transmettre un signalement fondé sur un traitement automatisé aux fins d'une action ultérieure, l'autorité compétente devrait examiner manuellement les données en même temps que d'autres informations afin de déterminer si la personne correspond au profil de risque et éliminer les faux positifs. Les destinataires des données doivent fournir un retour d'information sur les mesures prises sur la base du signalement.

Les données traitées doivent être précises et fiables

Les recherches de la FRA confirment que les systèmes d'information à grande échelle existants contiennent une quantité importante de données inexactes [49]. Des **données inexactes ou peu fiables** peuvent avoir des effets négatifs multiples dans le cadre du profilage algorithmique à des fins de gestion des frontières ou à des fins répressives. Des données inexactes peuvent avoir une incidence négative sur les individus, mais également donner lieu à des corrélations incorrectes et à une image faussée, compromettant ainsi l'efficacité des activités de la police et de la gestion des frontières.

Cela est particulièrement important dans les cas de données saisies par les citoyens, comme dans les données PNR et les demandes ETIAS, qui peuvent être plus enclines aux erreurs que les données officielles. De même, le filtrage des comptes de réseaux sociaux, qui est prévu par certains systèmes d'autorisation de voyage en dehors de l'UE, comporte un risque élevé d'introduire des informations peu fiables dans le processus de profilage. Il comporte par ailleurs un risque particulier de collecte d'informations révélant des informations sensibles à caractère personnel protégées par la Charte, telles que des opinions politiques ou des informations relatives à la vie sexuelle. Il est donc important de :

- fournir aux personnes des informations précises sur la collecte, le stockage et le traitement de leurs données et sur les principes applicables en matière de protection des données. Les individus devraient être informés de leurs droits, y compris des mécanismes de recours à leur disposition ;

- permettre aux personnes de rectifier leurs données lorsque les données sont inexactes, et d'être informées de la rectification ou de l'effacement des données ;

- prévoir des voies de recours administratifs et judiciaires efficaces en cas de violation des droits relatifs à la protection des données, y compris en cas de refus d'accès ou de refus de rectification ou d'effacement des données inexactes.

49 Voir FRA (2018c), p. 81-98.

Conclusion

Le profilage est un outil légitime utilisé par les agents de police et les gardes-frontières pour prévenir les activités criminelles, enquêter sur celles-ci et poursuivre leurs auteurs, ainsi que pour prévenir et détecter l'immigration irrégulière.

Pour être licite, équitable et efficace, le profilage doit être utilisé dans les limites fixées par la loi. Plus particulièrement, le profilage doit respecter les exigences en matière d'égalité de traitement et de protection des données à caractère personnel.

Cet objectif sera atteint par une combinaison d'éléments. Tout profilage doit :

- traiter les personnes sur un pied d'égalité, avec respect et dignité ;
- éviter de profiler les personnes sur la base d'un préjugé ;
- être raisonnable, objectif et fondé sur le renseignement ; et
- protéger de manière adéquate les données à caractère personnel et la vie privée des individus.

Différents outils sont mis à la disposition des agents de police et des gardes-frontières pour veiller à ce que ces principes soient connus, compris et respectés dans la pratique :

- avant de procéder au profilage, les agents devraient recevoir une orientation et une formation ;
- pendant le profilage, les détails de l'activité doivent être consignés et conservés ;
- après le profilage, les actions des agents devraient faire l'objet d'un suivi et être évaluées afin de déterminer les points d'amélioration.

Éviter le profilage illicite permettra non seulement aux agents de police et aux gardes-frontières de se conformer à la loi, mais contribuera également à ce que leurs actions soient comprises et acceptées par le grand public. Le renforcement de la confiance dans l'application de la loi et dans la gestion des frontières améliore l'efficacité des activités de la police et de la gestion des frontières et contribue ainsi à accroître les niveaux de sécurité et de sûreté au sein de la société dans son ensemble.

Annexe

Tableau 7 : Systèmes d'information à grande échelle existants et prévus dans l'UE

Système informatique	Objectif principal	Champ d'application personnel	Applicabilité	Instrument juridique/ proposition	Éléments d'identification biométriques
Système européen de comparaison des empreintes digitales (Eurodac)	Déterminer l'État membre responsable de l'examen d'une demande de protection internationale *Contribuer au contrôle de l'immigration irrégulière et des mouvements secondaires*	Demandeurs et bénéficiaires d'une protection internationale, *migrants en situation irrégulière*	28 EMUE + EAS	Règlement (UE) nº 603/2013 (règlement Eurodac) *COM(2016) 272 final (proposition Eurodac)*	
Système d'information sur les visas (VIS)	Faciliter l'échange de données entre les États membres Schengen sur les demandes de visa	Demandeurs de visa et regroupants	24 EMUE (excepté CY, HR, IE, UK) [1] + EAS	Règlement nº 767/2008/CE (règlement VIS)	
Système d'information Schengen (SIS II) — police	Garantir la sécurité dans l'UE et les États membres de l'espace Schengen	Personnes disparues ou recherchées	26 EMUE (excepté CY, IE) [2] + EAS	Décision 2007/533/JAI du Conseil (décision SIS II) *COM(2016) 883 final (proposition concernant l'utilisation de SIS II dans le domaine de la police)*	
Système d'information Schengen (SIS II) — frontières	Introduire et traiter des signalements aux fins de non-admission ou d'interdiction de séjour dans les États membres Schengen	Migrants en situation irrégulière	25 EMUE (excepté CY, IE, UK) [2] + EAS	Règlement (CE) nº 1987/2006 (règlement SIS II) *COM(2016) 882 final (proposition concernant l'utilisation de SIS II dans le domaine des frontières)*	

Système d'information Schengen (SIS II) — retour	*Introduire et traiter les signalements pour les ressortissants de pays tiers faisant l'objet d'une décision de retour*	*Migrants en situation irrégulière*	*25 EMUE (excepté CY, IE, UK)* [2] *+ EAS*	*COM(2016) 881 final (proposition concernant l'utilisation de SIS II dans le domaine du retour)*	
Système d'entrée/ sortie (EES)	*Calcul et suivi de la durée du séjour autorisé des ressortissants de pays tiers et recensement des personnes ayant dépassé la durée de séjour autorisée*	*Voyageurs arrivant pour un séjour de courte durée*	*22 EMUE (excepté BG, CY, HR, IE, RO, UK)* [3] *+ EAS*	*Règlement (UE) 2017/2226 (règlement EES)*	
Système européen d'information et d'autorisation concernant les voyages (ETIAS)	*Évaluer si un ressortissant d'un pays tiers sans visa pose un risque en matière de sécurité, d'immigration irrégulière ou de santé publique*	*Voyageurs sans visa*	*26 EMUE (excepté IE, UK)* [3] *+ EAS*	*COM(2016) 731 final (proposition ETIAS)*	*Aucun*
Système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN)	*Partager des informations sur les condamnations antérieures de ressortissants de pays tiers*	*Ressortissants de pays tiers ayant un casier judiciaire*	*27 EMUE (excepté DK)* [4]	*COM(2017) 344 final (proposition ECRIS-TCN)*	

Interopérabilité — Répertoire commun de données d'identité	*Établir un cadre pour l'interopérabilité entre EES, VIS, ETIAS, Eurodac, SIS II et ECRIS-TCN.*	*Ressortissants de pays tiers couverts par Eurodac, VIS, SIS II, EES, ETIAS et ECRIS-TCN*	*28 EMUE [5] + EAS*	*COM(2017) 793 final (proposition relative à l'interopérabilité dans le domaine des frontières et des visas)* *COM(2017) 794 final (proposition relative à l'interopérabilité dans le domaine de la coopération policière, asile et migration)*	

Remarque : Les systèmes et les changements prévus au sein des systèmes sont en italique ou sur fond bleu clair.

empreintes digitales ; empreinte palmaire ; image faciale ; profil ADN.

EMUE : États membres de l'UE.

EAS : les États associés à l'espace Schengen, à savoir l'Islande, le Liechtenstein, la Norvège et la Suisse.

1 *L'Irlande et le Royaume-Uni ne participent pas au VIS. Le Danemark n'est pas lié par le règlement, mais a adhéré au VIS. Le VIS ne s'applique pas encore à la Croatie et à Chypre et ne s'applique qu'en partie à la Bulgarie et à la Roumanie conformément à la décision (UE) 2017/1908 du Conseil du 12 octobre 2017.*

2 *Chypre et l'Irlande ne sont pas encore connectés au SIS. Le Danemark n'est pas lié par le règlement ou la décision du Conseil, mais a opté pour le SIS II et doit décider s'il y a lieu de procéder à nouveau à l'adoption des propositions du SIS II. Le Royaume-Uni participe au SIS, mais ne peut ni utiliser ni avoir accès à des signalements aux fins de non-admission ou d'interdiction de séjour dans l'espace Schengen. La Bulgarie, la Croatie et la Roumanie ne peuvent pas émettre de signalements à l'échelle de Schengen en vue de refuser l'entrée ou le séjour dans l'espace Schengen, étant donné qu'elles ne font pas encore partie de l'espace Schengen.*

3 *Le Danemark peut décider d'adhérer à l'EES et l'ETIAS.*

4 *Le système ECRIS-TCN ne s'applique pas au Danemark. Le Royaume-Uni et l'Irlande peuvent décider d'y adhérer.*

5 *Le Danemark, l'Irlande et le Royaume-Uni y participeront, étant donné qu'ils participent aux activités visant l'interopérabilité des systèmes informatiques.*

Source : FRA, sur la base des instruments juridiques existants et proposés (2018).

Références

Agence européenne de garde-frontières et de garde-côtes (Frontex) (2012), Common core curriculum, EU border guard basic training, mars 2012.

Agence européenne de garde-frontières et de garde-côtes (Frontex) (2013), Fundamental rights training for border guards, Trainers' Manual, 2013.

Agence européenne de garde-frontières et de garde-côtes (Frontex) (2015), Twelve seconds to decide — In search of excellence : Frontex and the principle of best practice, 2015.

Agence européenne de garde-frontières et de garde-côtes (Frontex) (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., et Bayerl, P. S. (2015), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, Butterworth-Heinemann, 2015.

American Civil Liberties Union (ACLU) (2016), « Eight Problems With Police "Threat Scores" », 13 janvier 2016.

Groupe de travail « article 29 » sur la protection des données (2014), Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, 536/14/EN, WP 211, Bruxelles, 27 février 2014.

Groupe de travail « article 29 » sur la protection des données (2017a), *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679*, WP 248 rév.01, 4 octobre 2017.

Groupe de travail « article 29 » sur la protection des données (2017b), Avis sur certaines questions clés de la directive police [(UE) 2016/680], 7 décembre 2017.

Groupe de travail « article 29 » sur la protection des données (2018a), Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251rév.01, 6 février 2018.

Groupe de travail « article 29 » sur la protection des données (2018b), Avis sur les propositions de règlement de la Commission portant établissement d'un cadre pour l'interopérabilité, WP266, Bruxelles, 23 avril 2018.

Belgique, Unia, Rapport annuel 2016, Bruxelles, septembre 2017.

Belgique, Unia, Rapport annuel — Convention entre Unia et la police fédérale — Budget 2015, Bruxelles, 2015.

Big Brother Watch, Smile you're on body worn camera Part II — Police, The use of body worn cameras by UK police forces, août 2017.

Body-Gendrot, S. (2016), « Making sense of French urban disorders in 2005 », *European Journal of Criminology*, vol. 13, nº 5, p. 556–572.

Bovens et al. (2014), « Public accountability » dans Bovens, M., Schillermans, T., et Goodlin, R. E. (éd.), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014), « Surveillance and system avoidance : criminal justice contact and institutional attachment », *American Sociological Review*, vol. 79, nº 3, p. 367–391.

Buolamwini, J., Gebru, T. (2018), Gender Shades : Intersectional Accuracy Disparities in Commercial Gender Classification, MIT Media Lab and Microsoft Research, 2018.

Centre d'analyse stratégique (2006), Enquête sur les violences urbaines — Comprendre les émeutes de novembre 2005 : les exemples d'Aulnay-sous-Bois et de Saint-Denis, Paris, La Documentation française, 2006.

Center on Privacy and Technology at Georgetown Law (2016), The perpetual line-up, unregulated police face recognition in America, 18 octobre 2016.

Coudert, F., Butin, D., et Le Metayer, D. (2015), « Body-worn cameras for police accountability : opportunities and risks », *Computer Law and Security Review*, vol. 31, p. 749–762.

Commission européenne (2017a), Hate crime training for law enforcement and criminal justice authorities : 10 key guiding principles, février 2017.

Commission européenne (2017b), Improving the recording of hate crime by law enforcement authorities — Key guiding principles, décembre 2017.

Commission européenne contre le racisme et l'intolérance (ECRI) (2007), Recommandation de politique générale nº 11 de l'ECRI sur la lutte contre le racisme et la discrimination dans les activités de la police adoptée le 29 juin 2007, Strasbourg, 4 octobre 2007.

Conseil de l'Europe, Comité des ministres (2001), Recommandation Rec(2001) 10 du Comité des ministres aux États membres sur le code européen d'éthique de la police adopté par le Comité des ministres, 19 septembre 2001.

Conseil de l'Union européenne (2009), Mise à jour du catalogue Schengen de l'UE relatif au contrôle des frontières extérieures, au retour et à la réadmission, 19 mars 2009.

Contrôleur européen de la protection des données (CEPD) (2015), Deuxième avis sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, avis nº 5/2015, Bruxelles, 24 septembre 2015.

Contrôleur européen de la protection des données (CEPD) (2018), Avis 4/2018 sur les propositions de deux règlements établissant un cadre d'interopérabilité entre les systèmes d'information à grande échelle de l'UE, Bruxelles, 18 avril 2018.

De Hert, P., et Lammerant, H. (2016), « Predictive profiling and its legal limits : effectiveness gone forever ? » dans van der Sloot, B., Broeders, D., et Schrijvers, E. (éd.), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, p. 145–173.

Défenseur des droits (2017), *Enquête sur l'accès aux droits.* — Volume 1 — Relations police/population : le cas des contrôles d'identité, 2017.

Dinant, J.-M., Lazaro, C., Poullet, Y., Lefever, N., et Rouvroy, A. (2008), Application of Convention 108 to the profiling mechanism — Some ideas for the future work of the consultative committee (T-PD), Doc. T-PD 01, p. 3.

États-Unis, GAO (General Accounting Office) (2000), *U.S. Customs Office: better targeting of airline passengers for personal searches could produce better results,* GAO/GGD-00-38, mars 2000.

Farrar, T. (2018), Self-awareness to being watched and socially-desirable behavior : A field experiment on the effect of body-worn cameras on police use-of-force, Police Foundation, 2018.

FRA (Agence des droits fondamentaux de l'Union européenne), Contrôleur européen de la protection des données (CEPD) et Conseil de l'Europe (2018), Handbook on European data protection law — 2018 edition, Luxembourg, Office des publications de l'Union européenne, mai 2018.

FRA (2013), Formation policière aux droits fondamentaux — Manuel à l'intention des formateurs de police, Luxembourg, Office des publications de l'Union européenne, décembre 2013.

FRA (2014a), Fundamental rights at airports : border checks at five international airports in the European Union, Luxembourg, Office des publications de l'Union européenne, 2014.

FRA (2014b), Fundamental rights at land borders : findings from selected European Union border crossing points, Luxembourg, Office des publications de l'Union européenne, 2014.

FRA (2014c), Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data, février 2014.

FRA (2016), *Rapport sur les droits fondamentaux 2016*, Luxembourg, Office des publications de l'Union européenne, 2016.

FRA (2017a), Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS), Avis FRA — 2/2017 [ETIAS], juin 2017.

FRA (2017b), Second European Union Minorities and Discrimination Survey — Main results, Luxembourg, Office des publications de l'Union européenne, décembre 2017.

FRA (2017c), Rapport sur les droits fondamentaux 2017, Luxembourg, Office des publications de l'Union européenne, mai 2017.

FRA (2016), EU-MIDIS II — Deuxième enquête de l'Union européenne sur les minorités et la discrimination — Les musulmans — Sélection de résultats, Luxembourg, Office des publications de l'Union européenne, septembre 2017.

FRA (2017e), Fundamental rights and the interoperability of EU information systems : borders and security, Luxembourg, Office des publications de l'Union européenne, mai 2017.

FRA (2018a), Interoperability and fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights, Avis de la FRA — 1/2018 [Interopérabilité], avril 2018.

FRA (2018b), #BigData : Discrimination in data-supported decision making, FRA Focus Paper, mai 2018.

FRA (2018c), Under watchful eyes : biometrics, EU IT-systems and fundamental rights, Luxembourg, Office des publications de l'Union européenne, février 2018.

FRA (2018d), Hate crime recording and data collection practice across the EU, Luxembourg, Office des publications de l'Union européenne, juin 2018.

FRA (2018e), Fundamental Rights Report 2018, Luxembourg, Office des publications de l'Union européenne, juin 2018.

FRA et Conseil de l'Europe (2018), Manuel de droit européen en matière de non-discrimination — Édition 2018, Luxembourg, Office des publications de l'Union européenne, février 2018.

France, ministère de l'intérieur (2018), Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale, 7 juin 2018.

Harcourt, B. (2004), « Rethinking Racial Profiling : A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally », *University of Chicago Law Review*, vol. 71, 2004.

Harris, D. (2002), « Flying While Arab: Lessons from the Racial Profiling Controversy », *Civil Rights Journal*, vol. 6, nº 1, hiver 2002.

Harris, D. (2003), *Profiles in Injustice; Why Racial Profiling Cannot Work*, The New Press, 2003.

Hildebrandt, M., et de Vries, K. (2013), *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*, New York, Routledge, 2013.

Hildebrandt, M., et Gutwirth, S. (éd.) (2008), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Berlin, Springer, 2008.

Hörnqvist, M. (2016), « Riots in the welfare state : The contours of a modern-day moral economy », *European Journal of Criminology*, vol. 13, nº 5, p. 573–589.

Hunt, P., Saunders, J., et Hollywood, J. S. (2014), *Evaluation of the Shreveport predictive policing experiment*, RAND Corporation, 2014.

Gandy, O. (2010), « Engaging rational discrimination : exploring reasons for placing regulatory constraints on decision support systems », *J Ethics Inf Technol*, vol. 12, nº 1, p. 29-42, 2010.

Gross, S. R. (2002), « Racial Profiling under Attack », D. Livingston, coauteur. *Colum. L.* Rev. 102, nº 5, p. 1413-38.

Jobard, F. (2008), « The 2005 French urban unrests: data-based interpretations », *Sociology Compass*, vol. 2, nº 4, p. 1287–1302.

Kádár, A., Körner, J., Moldova, Z., et Tóth, B. (2008), Control(led) group — Final report on the strategies for effective police stop and search (STEPSS) project, Budapest, p. 23.

Keskinen, S., et al. (2018), The stopped — Ethnic profiling in Finland, Swedish School of Social Science, University of Helsinki, Helsinki, 3 avril 2018.

Korff, D. (2015), *Passenger Name Records, data mining & data protection : the need for strong safeguards*, T-PD(2015)11, Strasbourg, 15 juin 2015.

Miller, J., et Alexandrou, B. (2016), *College of policing stop and search training experiment: Impact evaluation*, College of Policing Limited, 2016.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., et Floridi, L. (2016), « The ethics of algorithms : Mapping the debate », *Big Data & Society*, 1er décembre 2016.

Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., Brantingham, P. J., *Randomized controlled field trials of predictive policing*, 15 janvier 2016.

Nations unies (ONU) (2007), *Rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme dans la lutte contre le terrorisme*, A/HRC/4/26, 29 janvier 2007.

Nisbet, R., Elder, J., et Miner, G. (2009), *Handbook of statistical analysis & data mining applications*, Sydney (Canada), Elsevier, 2009.

Observatoire européen des phénomènes racistes et xénophobes (2016), Perceptions de la discrimination et de l'islamophobie : points de vue de membres des communautés musulmanes dans l'Union européenne, 2006.

Open Society Justice Initiative (2018a), *Regulating police stop and search: an evaluation of the reasonable grounds panel*, décembre 2018

Open Society Justice Initiative (2018b), *The recording of police stops: methods and issues*, décembre 2018.

Oswald, M., Grace, J., Urwin, S., et Barnes, G., « Algorithmic risk assessment policing models : lessons from the Durham HART model and 'experimental' proportionality », Information & Communications Technology Law, 31 août 2017.

Réseau européen d'experts juridiques dans la domaine de l'égalité des genres et de la non-discrimination (2016), Links between migration and discrimination — A legal analysis of the situation in EU Member States, juillet 2016.

Schauer, F. (2003), *Profiles Probabilities and Stereotypes*, Cambridge (MA), The Belknap Press of Harvard University Press, 2003.

Scheinin, M. (2007), rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme dans la lutte contre le terrorisme, *Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, Doc.NU A/HRC/4/26, 29 janvier 2007.

The Guardian (2015), « Northamptonshire police ban stop and search by officers who abuse powers », 18 août 2015.

Haut-Commissariat des Nations unies aux droits de l'homme (HCDH) (2014), Principes et directives recommandés sur les droits de l'homme aux frontières internationales, 23 juillet 2014.

Tóth, B. M., et Kádár, A. (2011), « Ethnic profiling in ID checks by the Hungarian police », *Policing and Society*, vol. 21, nº 4, p. 383–394.

Royaume-Uni, Camden and London Prepared (2006), Major Incident Procedures, What businesses and the voluntary sector need to know, avril 2006.

Royaume-Uni, College of Policing (2016), *Stop and Search*, Authorised Professional Practice (APP), 29 septembre 2016.

Royaume-Uni, Equality and Human Rights Commission (2009), *Police and racism : what has been achieved 10 years after the Stephen Lawrence Inquiry report?*, 2009.

Royaume-Uni, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), Stop and Search Powers : Are the police using them effectively and fairly?, 2013.

Royaume-Uni, Her Majesty's Inspectorate of Constabulary (HMIC) (2016), PEEL : Police legitimacy 2015 — An inspection of West Midlands Police, février 2016.

Royaume-Uni, Home Office (1999), The Stephen Lawrence Inquiry. — Report of An Inquiry by Sir William Macpherson of Cluny, février 1999.

Royaume-Uni, Home Office (2014a), CODE A : Revised code of practice for the exercise by: police officers of statutory powers of stop and search — Police officers and police staff of requirements to record public encounters, Norwich, The Stationery Office (TSO), 2014.

Royaume-Uni, Home Office (2014b), Best use of stop and search scheme, 2014.

Royaume-Uni, House of Commons Home Affairs Committee (2009), The Macpherson Report — Ten Years On, Twelfth Report of Session 2008–09, 22 juillet 2009.

Royaume-Uni, House of Lords (2006), Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) v. Commissioner of Police for the Metropolis and another (Respondents), [2006] UKHL 12, 8 mars 2006.

Royaume-Uni, London School of Economics (2011), Reading the Riots, décembre 2011.

Royaume-Uni, National Policing Improvement Agency (NPIA) (2012), Stop and search, the use of intelligence and geographic targeting, Findings from case study research, 2012.

Royaume-Uni, Northamptonshire Police (2018), Get Involved — Reasonable Grounds Panel, consulté en avril 2018.

Royaume-Uni, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015), An Independent Report into Stop & Search Encounters by Staffordshire Police, janvier 2015.

Royaume-Uni, Stop Watch (2011), "Carry on Recording" Why police stops should still be recorded, mai 2011.

Royaume-Uni, West Midlands Police (2012), Stop and Search Policy, novembre 2012.

Royaume-Uni, West Midlands Police (2016), Stop and Search Recommendations, juillet 2015 (dernière modification en juin 2016).

Royaume-Uni, West Midlands Police (2017a), Stop and Search in the West Midlands: Presentation to Den Hague City Council, avril 2017.

Royaume-Uni, West Midlands Police (2017b), New "app" set to speed up Stop & Search process, août 2017.

Royaume-Uni, West Midlands Police (2018), Stop and Search Scrutiny Panels, consulté en avril 2018.

Royaume-Uni, West Midlands Police and Crime Commissioner (2014), Stop and Search Action Plan — Outcome of consultation, janvier 2014.

Van Brakel, R. (2016), « Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing » dans van der Sloot, B., Broeders, D., et Schrijvers, E. (éd.), Conseil scientifique néerlandais pour la politique gouvernementale (*Wetenschappelijke Raad voor het Regeringsbeleid*), *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, p. 117–141.

Wrench, J. (2007), *Diversity management and discrimination: immigrants and ethnic minorities in the EU*, Aldershot, Ashgate, 2007.

Zarsky, T. Z. (2011), « Governmental Data Mining and its Alternatives », *Penn State Law Review*, vol. 11, nº 2, p. 285–330.

Législation de l'Union européenne

Droits fondamentaux

Charte des droits fondamentaux de l'Union européenne, 2012/C 326/02, JO 2012 C 326.

Explications relatives à la Charte des droits fondamentaux, 2007/C 303/02, JO 2007 C 303/17.

Non-discrimination

Directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement.

Directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail.

Protection des données

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

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Gestion des frontières

Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO 2007 L 205/63.

Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JO 2016 L 119/132.

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), JO 2006 L 381/4.

Règlement (CE) nº 767/2008 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), JO 2008 L 218/60.

Règlement (UE) nº 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) nº 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, JO 2013 L 180/1.

Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil, et abrogeant le règlement (CE) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil, JO 2016 L 251/1.

Règlement (UE) nº 1052/2013 du Parlement européen et du Conseil du 22 octobre 2013 portant création du système européen de surveillance des frontières (Eurosur), JO 2013 L 295/11.

Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), JO 2016 L 77/1.

Jurisprudence

France, Cour de cassation, Décision 1245, 9 novembre 2016.

Royaume-Uni, House of Lords, *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.,* [2006] UKHL 12, 8 mars 2006.

CJUE, C-524/06, Heinz Huber c. Bundesrepublik Deutschland, 16 décembre 2008.

CouEDH, *B.S. c. Espagne*, requête nº 47159/08, 24 juillet 2012.

CouEDH, *S. et Marper c. Royaume-Uni*, requêtes nos 30562/04 et 30566/04, 4 décembre 2008.

CouEDH, *Gillan et Quinton c. Royaume-Uni*, requête nº 4158/05 2010, 12 janvier 2010.

Conseil des droits de l'homme des Nations unies, *Rosalind Williams Lecraft c. Espagne*, Comm. nº 1493/2006, 30 juillet 2009.

Comment prendre contact avec l'Union européenne?

En personne

Dans toute l'Union européenne, des centaines de centres d'information Europe Direct sont à votre disposition. Pour connaître l'adresse du centre le plus proche, visitez la page suivante: https://europa.eu/european-union/contact_fr

Par téléphone ou courrier électronique

Europe Direct est un service qui répond à vos questions sur l'Union européenne. Vous pouvez prendre contact avec ce service:

- par téléphone:
  - via un numéro gratuit: 00 800 6 7 8 9 10 11 (certains opérateurs facturent cependant ces appels),
  - au numéro de standard suivant: +32 22999696 ;
- par courrier électronique via la page https://europa.eu/european-union/contact_fr

Comment trouver des informations sur l'Union européenne?

En ligne

Des informations sur l'Union européenne sont disponibles, dans toutes les langues officielles de l'UE, sur le site internet Europa à l'adresse https://europa.eu/european-union/index_fr

Publications de l'Union européenne

Vous pouvez télécharger ou commander des publications gratuites et payantes à l'adresse https://publications.europa.eu/fr/publications. Vous pouvez obtenir plusieurs exemplaires de publications gratuites en contactant Europe Direct ou votre centre d'information local (https://europa.eu/european-union/contact_fr).

Droit de l'Union européenne et documents connexes

Pour accéder aux informations juridiques de l'Union, y compris à l'ensemble du droit de l'UE depuis 1952 dans toutes les versions linguistiques officielles, consultez EUR-Lex à l'adresse suivante: http://eur-lex.europa.eu

Données ouvertes de l'Union européenne

Le portail des données ouvertes de l'Union européenne (http://data.europa.eu/euodp/fr) donne accès à des ensembles de données provenant de l'UE. Les données peuvent être téléchargées et réutilisées gratuitement, à des fins commerciales ou non commerciales.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Les progrès technologiques ont contribué à un recours accru au profilage dans un large éventail de contextes, et l'utilisation des outils de profilage pour soutenir le travail des agents de police et de la gestion des frontières a récemment fait l'objet d'une plus grande attention de la part des États membres de l'UE. Le profilage est légitimement utilisé pour prévenir, instruire et poursuivre les infractions pénales, ainsi que pour prévenir et détecter l'immigration irrégulière. Mais le profilage illicite peut saper la confiance dans les autorités et stigmatiser certaines communautés.

Le présent guide explique le profilage, les cadres juridiques qui le régissent et les raisons pour lesquelles le profilage licite est à la fois nécessaire pour garantir le respect des droits fondamentaux et essentiel à l'efficacité des opérations de police et de gestion des frontières. Le guide fournit également des orientations pratiques quant à la manière d'éviter tout profilage illicite dans les opérations de police et de gestion des frontières.

FRA – AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tél. + 43 (1) 580 30-0 – Fax + 43 (1) 580 30-699
fra.europa.eu – info@fra.europa.eu
@EURightsAgency

Office des publications
de l'Union européenne