COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 18 mai 2017 T-PD (2016)02rev5

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

Projet de guide pratique sur l'utilisation de données à caractère personnel par la police

Direction générale Droits de l'Homme et État de droit

Introduction

La Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel par la police énonce un ensemble général de principes à appliquer dans ce secteur pour garantir le respect du droit à la protection des données et de la vie privée prévu par l'article 8 de la Convention européenne des droits de l'homme et par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »).

Depuis son adoption, la Recommandation (87)15 a fait l'objet de plusieurs évaluations (en 1993, 1998 et 2002), sur le plan tant de sa mise en œuvre que de sa pertinence. En 2010, le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a décidé de réaliser une étude[1] sur l'utilisation de données à caractère personnel par la police dans l'ensemble de l'Europe. Cette évaluation a montré que les principes de la Recommandation (87)15 constituaient un point de départ approprié pour élaborer des réglementations s'appliquant à cette question au niveau local et que l'élaboration d'un guide pratique sur l'utilisation de données à caractère personnel par la police, sur la base des principes énoncés par la recommandation, fournirait des éléments d'orientation clairs et concrets sur ce que ces principes impliquent au niveau opérationnel.

Le présent guide a donc été élaboré à cette fin. Il vise à mettre en évidence les problèmes les plus importants qui peuvent découler de l'utilisation de données à caractère personnel par la police et signale les principaux éléments à prendre en compte dans ce contexte.

Ce guide ne reproduit ni les dispositions de la Convention 108 ni celles de la Recommandation (87)15 mais se concentre sur leur application pratique.

Ces principes généraux et leurs conséquences pratiques visent à ce qu'un juste équilibre soit trouvé entre différents intérêts durant le travail de la police, tels que la sûreté ou la sécurité publique, ainsi que le respect des droits des personnes à la protection de la vie privée et à la protection des données.

Pour faciliter la lecture du présent guide, un glossaire des termes utilisés est fourni à la fin du document.

[1] Voir le rapport « Twenty–five years down the line » de Joseph A. Cannataci.

Le traitement de données devrait être entièrement conforme aux principes de nécessité, de proportionnalité et de limitation de la finalité. Cela signifie qu'il ne devrait être effectué par la police que dans un but prédéfini, précis et légitime, qu'il devrait être nécessaire et proportionné à ces fins légitimes, et qu'il devrait toujours être compatible avec la finalité initialement poursuivie. Il faudrait en outre que ce traitement soit assuré de façon loyale, transparente et licite, et qu'il soit adéquat, pertinent et non excessif par rapport aux finalités. Enfin, les données traitées par la police devraient être exactes et actualisées pour que leur qualité soit optimale.

1. Champ d'application

Les principes énoncés dans le présent guide s'appliquent au traitement de données à caractère personnel à des fins policières, plus précisément aux fins de prévention, d'investigation et de répression des infractions pénales et d'exécution des sanctions pénales. Le terme « police » utilisé dans le texte désigne plus généralement les services chargés de l'application de la loi et/ou d'autres organes publics et/ou entités privées autorisés par la loi à traiter des données à caractère personnel pour les mêmes fins.

2. Collecte et utilisation des données

Le traitement de données à caractère personnel à des fins policières devrait se limiter à ce qui est nécessaire à la prévention, l'investigation et la répression d'infractions pénales ainsi qu'à l'exécution de sanctions pénales (pour une infraction pénale déterminée par exemple).

Le traitement des données à caractère personnel à des fins policières constitue une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel et toute ingérence doit par conséquent être fondée sur des dispositions légales (claires et publiquement disponibles), poursuivre un but légitime et se limiter à ce qui est nécessaire pour atteindre le but poursuivi.

Il importe que la collecte de données à caractère personnel par la police soit conforme au cadre législatif et toujours liée à des enquêtes en cours. Avant et pendant la collecte des données à caractère personnel, il faudrait toujours se demander si de telles données collectées sont nécessaires à l'enquête. Au stade de la collecte, toute donnée à caractère personnel « utile » peut être traitée à condition que toutes les obligations légales la concernant soient respectées. Après la collecte, il faut impérativement procéder à une analyse approfondie pour évaluer quelles sont les données qui doivent être conservées et celles qui doivent être effacées.

La police devrait appliquer le principe de minimisation des données à toutes les étapes du traitement et ne devrait pas continuer à traiter des données qui ne correspondent pas à la finalité poursuivie. Les données à caractère personnel qui sont collectées à un stade initial de l'enquête et pour lesquelles il est par la suite établi au cours de l'enquête qu'elles ne sont plus pertinentes ne devraient plus être traitées (par exemple, lorsque l'innocence d'un suspect est confirmée).

Avant de procéder à la collecte de données à caractère personnel, il convient de se poser les questions suivantes : « Pour quelle raison l'obtention de ces données est-elle nécessaire ? », « Quel est exactement le but poursuivi ? ».

Exemple : en cas d'écoutes téléphoniques, les services de répression ne devraient demander que le(s) numéro(s) nécessaire(s) à la période qui fait l'objet de l'enquête et uniquement pour la ou les personnes concernées. Une liste des numéros de téléphone de la ou des personnes impliquées dans l'infraction présumée peut être obtenue s'il existe des éléments qui indiquent que ces données peuvent servir à l'enquête, mais celles-ci ne peuvent pas être conservées ou traitées si l'analyse montre qu'elles ne sont pas strictement nécessaires pour la finalité de l'enquête.

Conformément au principe de limitation de la finalité, les données à caractère personnel collectées à des fins policières doivent servir exclusivement à de telles fins et ne doivent pas être utilisées d'une manière qui soit incompatible avec cette finalité, sauf disposition contraire de la législation nationale.

Exemple : les données collectées par la police dans le cadre d'une enquête ne peuvent pas être utilisées pour déterminer l'affiliation politique de la personne concernée.

3. Utilisation ultérieure des données

Tout traitement ultérieur de données par la police doit respecter les mêmes obligations légales que celles qui s'appliquent au traitement de données à caractère personnel : il devrait être prévu par la loi, être nécessaire et proportionné au but légitime poursuivi.

Comme les données à caractère personnel collectées dans une finalité précise peuvent être très facilement utilisées pour une autre finalité, les données d'une personne recueillies à des fins policières ne devraient pas être conservées et traitées d'une façon non structurée, sauf s'il existe une base légale et une justification opérationnelle à cela. La règle générale est que toutes les données détenues par la police doivent avoir un lien direct avec l'enquête et doivent être traitées en cohérence avec cette enquête spécifique. Cependant, dans des cas exceptionnels dans lesquels un critère supplémentaire vient valider la légitimité du traitement, les données peuvent être conservées dans une forme structurée plus souple. Par exemple, les données de récidivistes ou les données relatives à des membres d'un groupe terroriste peuvent être conservées plus longtemps et dans une forme structurée plus souple au vu du type d'infraction pour lesquelles ils sont poursuivis ou condamnés. Toutefois, même dans ces cas, l'utilisation ultérieure des données à caractère personnel, en particulier de personnes vulnérables, telles que les victimes, les mineurs, les personnes handicapées, les personnes en difficulté ou bénéficiant d'une protection internationale, devrait être fondée sur des bases légales solides et faire l'objet d'un examen approfondi.

Dans des affaires difficiles concernant la traite des êtres humains, le trafic de drogue, l'exploitation sexuelle, etc., dans lesquelles les victimes peuvent souvent aussi être également des suspects et où la protection des victimes d'un crime plus grave peut l'emporter sur l'intérêt de poursuivre des crimes moins graves, il est conseillé aux services de police de se référer aux bonnes pratiques internationales et d'améliorer la façon dont ils échangent des informations sur la question avec d'autres services de police.

Exemple : les données biométriques recueillies à des fins d'immigration peuvent être traitées, si la loi l'autorise, pour d'autres utilisations répressives (telles que les contrôles des personnes recherchées pour un crime ou un acte terroriste grave). À l'inverse, pour les vols mineurs (tels que le vol d'une revue), les recherches dans le fichier ADN détenu à des fins d'immigration ne seront pas considérées comme appropriées et pourraient pas ailleurs ne pas satisfaire le principe de proportionnalité.

4. Information des personnes concernées

L'une des obligations les plus importantes du responsable du traitement des données est de fournir des informations sur le traitement de leurs données aux personnes concernées. Il s'agit d'une double obligation : 1) le responsable du traitement communique des informations générales sur le traitement des données qu'il effectue et 2) il donne aux intéressés qui en font la demande des informations spécifiques sur le traitement de leurs données à caractère personnel.

L'obligation générale suppose que, en principe, les personnes concernées reçoivent un certain nombre de renseignements avant le traitement des données, notamment le nom et les coordonnées du responsable du traitement, du sous-traitant et des destinataires, mais aussi des informations relatives à l'ensemble de données à traiter, la finalité du traitement des données, la base légale de ce traitement ainsi que des informations sur leurs droits. Il appartient à ceux qui communiquent ces informations de respecter un juste équilibre entre tous les intérêts concernés et de tenir compte de la nature particulière des fichiers ad hoc ou provisoires et des autres fichiers particulièrement sensibles, tels que les fichiers de renseignement en matière pénale, afin d'éviter de porter gravement préjudice à la police dans l'exercice de ses fonctions.

Les informations données de façon générale au public dans son ensemble devraient permettre de promouvoir leur sensibilisation, de les informer de leurs droits et des modalités de leur exercice. Les informations fournies devraient également préciser dans quelles conditions les droits des intéressés peuvent faire l'objet d'exceptions et comment ces personnes peuvent former un recours contre une décision prise, suite à une demande de leur part, par le responsable du traitement des données en réponse à leur demande.

Les sites internet et tout autre média facilement accessible peuvent jouer un rôle dans l'information du public. Il est recommandé, en guise de bonne pratique, de mettre des lettres-types à la disposition des personnes concernées qui souhaitent exercer leurs droits. Il devrait être de la responsabilité du responsable du traitement ou du sous-traitant de fournir une information qui met en lumière la protection des données et les droits des personnes concernées.

Conformément à la seconde obligation consistant à donner des informations spécifiques relatives à ses données à la personne concernée, il appartient au responsable du traitement de l'informer, sur demande, des activités de traitement réalisées sur ses données. En clair, cela signifie que si une personne voit ses données collectées au cours d'une enquête, la police doit lui communiquer, dès que les circonstances le permettent, les informations sur les activités de traitement de ses données. La communication de ces informations à la personne concernée peut être effectuée telle qu'elle est prévue dans le droit interne. Les informations doivent être communiquées de manière claire et intelligible.

Il convient toutefois de souligner que la police n'a pas à faire cette démarche si elle estime que la communication de cette information à l'intéressé peut être préjudiciable à l'enquête, par exemple parce qu'elle lui permettra de prendre la fuite ou de détruire des éléments de preuve. La non-communication d'informations sur le traitement des données ne doit être utilisée que de façon limitée et seulement lorsqu'elle peut être clairement justifiée.

Exemple : pour procéder à la surveillance discrète d'un délinquant sexuel à haut risque, il peut être parfaitement justifié de ne pas communiquer à l'intéressé des informations sur le traitement de ses données et la conservation prolongée de celles-ci, dans la mesure où ces données sont nécessaires à cette fin, si l'on considère que ces informations peuvent nuire à l'enquête.

5. Exceptions

Les exceptions ne peuvent être utilisées que si elles sont prévues par la loi et constituent une mesure nécessaire et proportionnée dans une société démocratique. Cela signifie que la mesure sur laquelle l'exception est fondée est publique, ouverte, transparente et suffisamment détaillée. En outre, l'exception ne peut être utilisée que pour les objectifs légitimes énumérés et uniquement lorsque cela est nécessaire et proportionné pour atteindre le but poursuivi. Enfin, les mesures utilisées doivent être soumises à un contrôle externe approprié.

Les exceptions peuvent être applicables aux principes décrits aux points 2, 3, 4, 7 ainsi qu'aux droits des personnes concernées (point 19) dans le cas de certaines activités spécifiques de traitement de données. Il s'agit principalement des activités menées dans le but d'assurer la sécurité nationale, la défense, la sûreté publique, la protection d'intérêts économiques et financiers importants, l'impartialité et l'indépendance de la justice ou la protection des droits et libertés fondamentales d'autrui.

Des exceptions à ces règles et principes peuvent également se justifier si leur exécution met en danger la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres objectifs essentiels d'intérêt général.

Exemple : si le fait de donner des informations à une personne concernée peut mettre en danger la sécurité d'un témoin ou d'un informateur, ce droit peut être limité.

Il est parfaitement légitime pour un État de protéger sa sécurité nationale et donc pour la police d'enquêter sur des personnes participant à des activités terroristes, mais cet objectif ne saurait justifier la décision de procéder à des écoutes téléphoniques permanentes, non contrôlées et illimitées du téléphone portable d'un individu (*affaire Zakharov c. Russie*[2]) ou d'utiliser des techniques d'enquête spéciales (point 6) uniquement contrôlées par le gouvernement (*affaire Szabó c. Hongrie*[3]).

Exemple : des données policières peuvent être échangées avec des services de sécurité nationale s'il existe une menace réelle et imminente pour la sécurité nationale, par exemple pour déjouer un attentat terroriste. Afin d'identifier rapidement l'auteur de l'attentat, la police doit coopérer activement

[2] CEDH Roman Zakharov v. Russie, 47143/06

[3] CEDH Szabó and Vissy v. Hongrie, 37138/14

avec les services de sécurité nationale et échanger les données à caractère personnel recueillies sur des suspects. Mais s'il n'y a pas de risque d'attentat terroriste, la police ne devrait pas communiquer ses données aux services de sécurité nationale car cela serait contraire au principe de la limitation de la finalité.

6. Utilisation de techniques d'enquête spéciales

La police devrait toujours choisir la ou les méthodes les plus efficaces et les plus simples pour une enquête. Les méthodes les moins intrusives, dans le cas où elles peuvent être employées pour aboutir au but recherché, devraient être privilégiées. L'emploi de techniques spéciales d'enquête ne peut être envisagé que si le même résultat ne peut être obtenu par des méthodes moins intrusives.

Les progrès techniques ont rendu la surveillance électronique plus facile, mais il ne faut pas oublier que leur utilisation est une ingérence dans le droit au respect de la vie privée, le droit à la protection des données à caractère personnel et d'autres droits fondamentaux. Le choix de la méthode d'enquête doit donc s'accompagner d'une réflexion sur des éléments tels que le rapport coût-efficacité, l'utilisation des ressources et l'efficacité.

Exemple : dans une enquête, les preuves de la communication entre deux suspects peuvent être recueillies de diverses façons. Si des interrogatoires, des témoignages ou une surveillance discrète permettent d'obtenir le même résultat sans nuire à l'efficacité de l'enquête, ces moyens doivent être préférés à l'utilisation de mesures de surveillance secrète.

7. Utilisation de nouvelles technologies de l'information

Lorsque de nouveaux moyens techniques de traitement des données deviennent opérationnels, il est conseillé de procéder à une analyse d'impact de la réglementation qui devrait tenir compte de la conformité des nouvelles mesures aux normes de protection de la vie privée et de protection des données.

Si le traitement est fortement susceptible de porter atteinte aux droits de l'intéressé(e), il appartient au responsable du traitement des données de procéder à une évaluation de l'impact sur la protection des données (EIPD), afin d'apprécier l'ensemble des risques que ce traitement présente pour les actions envisagées. Il est recommandé que l'évaluation des risques ne soit pas statique, mais continue (c'est-à-dire effectuée à des intervalles raisonnables), et vise chacune des étapes de l'activité de traitement des données. La pertinence de l'EIPD doit être contrôlée à intervalles raisonnables.

Exemple :les nouvelles techniques de *data mining* peuvent offrir des possibilités étendues pour l'identification d'éventuels suspects et il convient d'évaluer soigneusement leur conformité avec la législation en vigueur en matière de protection des données.

L'autorité de contrôle a un rôle important à jouer ; elle doit signaler les risques que ce traitement automatisé présente pour la protection des données et présenter les garanties à mettre en place pour que tous les moyens techniques soient conformes à la législation sur la protection des données. Cependant, la police n'est pas tenue de s'adresser à l'autorité de contrôle à chaque fois qu'elle met en place de nouvelles technologies. Elle peut le faire si l'EIPD a démontré l'existence d'un risque élevé d'atteinte aux droits de l'intéressé.

Au cours de la procédure d'échange avec l'autorité de contrôle, l'accent devrait être mis sur l'atténuation des effets négatifs spécifiques que le traitement des données pourrait produire sur le droit à protection de la vie privée et le droit à la protection des données.

Les consultations entre l'autorité de contrôle et le responsable du traitement des données devraient avoir lieu dans un cadre qui permet suffisamment à cette autorité de donner un avis motivé et une évaluation des activités du responsable du traitement des données sans compromettre ses fonctions essentielles.

À l'issue de ces consultations, le responsable du traitement devrait mettre en œuvre les mesures et les garanties nécessaires convenues avant de procéder au traitement des données.

Exemple : la mise en place d'un système de reconnaissance faciale automatique devrait faire l'objet de consultations pour que les risques encourus par les droits de l'intéressé soient clairement indiqués. S'il le faut, des garanties spécifiques devraient être mises en place (concernant la durée de conservation des données, les fonctionnalités de correspondance croisée, le lieu de stockage des données et les problèmes d'accès aux données, etc.) pour se conformer aux principes et dispositions de la protection des données

Il convient, pendant le processus de consultation, de communiquer des renseignements appropriés à l'autorité de contrôle, notamment en ce qui concerne le type de fichier, le responsable du traitement des données, le sous-traitant, la base légale et la finalité du traitement des données, le type de données qui figurent dans le fichier et les destinataires des données. Il faut également fournir des informations sur la conservation des données et la politique applicable en matière d'enregistrement et d'accès.

Exemple : les fichiers nationaux de référence qui contiennent des données sur les empreintes digitales doivent être conformes à la législation nationale. Toute information détaillée sur les fichiers, tel que leur finalité ou le responsable du traitement des données, etc., devrait être indiquée ou mise à disposition de l'autorité de contrôle.

Utilisation de l'internet des objets dans le travail de police

Les données transmises à la police et à ses agents ou par ceux-ci dans le cadre de leurs activités opérationnelles (par exemple, au moyen d'un GPS et de caméras corporelles) par internet montrent que la technologie de l'internet des objets est déjà opérationnelle. En raison des vulnérabilités qu'elle peut présenter, cette technologie exige de prendre des mesures telles que l'authentification des données, le contrôle de l'accès pour assurer la sécurité des données et la protection des données pour résister aux cyber-attaques.

Exemple : compte tenu de possibles problèmes de sécurité, les « lunettes intelligentes » utilisées par la police ne doivent pas être directement liées à une base de données nationale des casiers judiciaires ; elles devraient recueillir des informations qui seront ensuite téléchargées dans un environnement informatique sécurisé pour analyses ultérieures.

Big data et profilage dans les services de police

Les avancées technologiques dans le domaine du traitement et de l'analyse d'ensembles de données importants et complexes qui donnent lieu à la création de mégadonnées (*big data*), ainsi que l'analyse de ces mégadonnées présentent aussi bien des occasions à saisir que des défis à relever pour les services de police qui décident d'utiliser des sources d'information numériques et des techniques de profilage pour accomplir leur mission judiciaire.

Les technologies du big data permettent la collecte et l'analyse d'une quantité massive de données générées par les communications et les dispositifs électroniques qui s'ajoutent à d'autres données de masse. Ce mode de traitement des données risque d'entraîner une ingérence collatérale qui peut avoir des répercussions sur les droits fondamentaux d'une personne, tel que le droit au respect de la vie privée et le droit à la protection des données

Les lignes directrices du Conseil de l'Europe sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère du big data[4] peuvent être également utiles dans le contexte de l'analyse de ces masses de données par la police.

Les technologies du big data et les techniques d'analyse de ces données peuvent contribuer à la détection d'une infraction, mais il est important de tenir compte des risques considérables que présente cette forme de traitement de données :

[4] Document T-PD(2017)1

- l'interprétation d'informations provenant de bases de données utilisées dans des domaines et contextes différents peut aboutir à des conclusions erronées qui peuvent avoir de graves conséquences pour les intéressés ;
- le profilage peut déboucher sur des conclusions discriminatoires, susceptibles de renforcer les préjugés, la stigmatisation et la discrimination;
- la quantité croissante de données détenues dans des bases de données peut entrainer une sévère vulnérabilité et par conséquent des risques de violation des données si la sécurité de ces informations n'est pas garantie.

Lorsque le traitement de big data s'appuie sur des données à caractère personnel, le responsable du traitement des données devrait tenir dûment compte des considérations suivantes :

- la vérification de l'exactitude, du contexte et de la pertinence des données s'impose ;
- leur utilisation exige une obligation de rendre des comptes ;
- leur utilisation doit être combinée avec les méthodes d'enquête traditionnelles ;
- leur utilisation est limitée à des formes graves de criminalité ;
- l'analyse prédictive nécessite notamment une intervention humaine pour évaluer la pertinence de l'analyse et des conclusions ;
- les lignes directrices en matière d'éthique élaborées au niveau national ou international devraient être prises en considération ;
- faire preuve de transparence et expliquer comment les données sont traitées dans le respect des principes applicables à la protection des données. Lorsque les données collectées dans un but précis sont utilisées dans un autre but compatible, il importe que l'organe responsable du traitement informe les personnes concernées de cette utilisation secondaire ;
- la légalité du traitement des données et sa conformité avec les conditions fixées par l'article 8 de la Convention européenne des droits de l'homme devraient être démontrées ;
- il importe de mettre en place une politique de sécurité des informations ;
- l'analyse du big data et le traitement des résultats de cette analyse devraient être effectués par des personnes expertes en la matière ;
- veiller à la loyauté du traitement des données à caractère personnel lorsque la prise de décisions qui ont des conséquences pour les intéressés repose sur l'utilisation du big data.

8. Traitement portant sur des catégories particulières de données

Les catégories spéciales de données telles que les données génétiques, les données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes, les données biométriques identifiant une personne, une donnée personnelle indiquant l'origine raciale et ethnique, les opinions politiques, l'appartenance à un syndicat, les croyances religieuses ou autres convictions ou donnant des indications sur la santé ou la vie sexuelle ne peuvent être traitées que si des protections supplémentaires sont prévues par la loi. Ces protections peuvent être de nature technique, comme par exemple des mesures de sécurité supplémentaires ou organisationnelle, tel que la mise en place d'un traitement de ces données à part et non dans l'environnement de traitement prévu pour les catégories de données « normales ».

Un juste équilibre des intérêts doit être trouvé pour déterminer si la police est autorisée à traiter des données sensibles et dans quelle mesure. Il est en outre recommandé d'utiliser davantage l'évaluation de l'impact sur le respect de la vie privée (EIPD) afin d'être sûr que des protections supplémentaires sont mises en place de manière adéquate. Le responsable du traitement devrait démontrer après évaluation que la finalité du traitement (p.ex. l'enquête pénale) ne peut pas être atteinte en utilisant un traitement qui affecte moins le droit au respect de la vie privée et le droit à la protection des données de la personne concernée, et que le traitement de catégories spéciales de données ne présente pas un risque de discrimination pour la personne concernée.

La collecte de données sur des personnes fondée seulement sur des données à caractère sensible qui ne serait pas prévue par la loi est interdite.

En ce qui concerne ces données (sensibles), le profilage devrait être évité en règle générale et ne devrait être autorisé que lorsque des garanties supplémentaires importantes sont mises en place pour contenir le risque potentiel de discrimination. Il peut s'agir notamment de mesures visant à éviter qu'une personne soit soupçonnée d'appartenir à une organisation criminelle parce qu'elle est

assimilée à tous les habitants d'un quartier où une organisation criminelle est active et où les habitants ont la même origine ethnique. Il faudrait d'autres critères supplémentaires tels que la communication fréquente avec des membres connus du groupe, etc., pour autoriser le traitement des données pour ce motif.

Exemple : le traitement de données pour des motifs purement religieux ne devrait pas être autorisé. Cependant, lors d'une enquête sur un groupe de personnes participant éventuellement à des activités terroristes associées à un groupe religieux particulier, il pourrait être important de traiter des données visant spécifiquement les adeptes de ce groupe religieux (liées au lieu de culte, aux prédicateurs religieux, aux coutumes, à l'enseignement, aux membres et à la structure de la communauté religieuse, etc.). Il sera néanmoins interdit de cibler tous les adeptes d'une religion, seulement sur la base de leur appartenance.

9. Conservation des données

Les données sont traitées tant qu'elles servent les fins pour lesquelles elles ont été collectées. Les données qui ne sont plus pertinentes de ce point de vue doivent être effacées, sauf si un traitement ultérieur est prévu par la loi *et* est considéré comme pertinent pour une fin qui n'est pas incompatible avec le but initial du traitement. Les données conservées devraient être adéquates, actualisées, nécessaires, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées.

Le classement des données à caractère personnel par la police devrait suivre une distinction claire entre les différentes catégories de personnes, par exemple les suspects, les personnes condamnées pour une infraction pénale, les victimes et les tiers tel que les témoins. Cette distinction devrait également tenir compte de la finalité précise des données collectées. Il convient de mettre en place des garanties pour les personnes qui ne sont pas soupçonnées d'infraction pénale ou qui n'ont pas été condamnées pour une infraction pénale.

Le principe de nécessité doit être appliqué tout au long du cycle de vie du traitement. Le stockage peut être autorisé si l'analyse montre que les données à caractère personnel sont strictement nécessaires pour atteindre l'objectif de l'enquête.

Les motifs de conservation et de traitement des données devraient être réexamines périodiquement. Il est à noter que le traitement des données à caractère personnel en dehors du délai légal prévu pour la conservation peut constituer une violation grave du droit à la protection de ces données et que les éléments de preuve recueillis ainsi peuvent être considérés comme illégaux.

Les périodes de conservation des données sont généralement réglementées dans le droit interne ou international. Pour être en conformité avec la législation tout en veillant à l'efficacité et à l'aboutissement d'une enquête, il est fortement recommandé aux services de police d'élaborer des procédures internes et/ou des recommandations sur la façon de réexaminer la période de conservation des données à caractère personnel. Par exemple, si la loi prescrit une durée de conservation des données de 4 ans mais que la personne ayant fait l'objet d'une enquête est acquittée au bout de 2 ans de toutes les charges qui pèsent contre elle, ses données sont effacées de la base de données (si elle n'est pas récidiviste ou si aucune autre information n'indique qu'elle a de nouveau commis un crime de la même catégorie). De même, s'il s'avère qu'au bout de 4 ans l'enquête est toujours en cours et que les données concernant cette personne restent pertinentes, la police devrait être en mesure de les conserver.

Dans ce dernier cas, il semble important d'élaborer la stratégie de conservation de telle sorte que les données utilisées dans les poursuites pénales restent à la disposition du responsable de traitement jusqu'à ce que la procédure judiciaire s'achève (c'est-à-dire toutes les voies de recours ont été épuisées ou tous les délais de recours sont expirés).

La police devrait prévoir des systèmes et des mécanismes pour veiller à ce que les données enregistrées soient exactes et que leur intégrité soit préservée.

Lors de l'élaboration de politiques internes, les obligations internationales qui imposent la transmission de données à des organes internationaux comme Europol, Eurojust et INTERPOL, ainsi que les accords bilatéraux et l'entraide judiciaire entre États membres et pays tiers, doivent être respectées.

Il convient de classer les données par catégorie en fonction de leur degré d'exactitude et de fiabilité afin d'aider la police dans ses activités. Il est recommandé d'utiliser des codes de traitement pour différencier ces catégories. L'utilisation d'un système de classification permet de faciliter l'appréciation de la qualité et de la fiabilité des données. La classification des données est également importante lorsqu'elles doivent être communiquées à d'autres services de police ou à d'autres États.

Exemple : les informations directement tirées des déclarations d'une personne seront évaluées différemment des informations collectées par ouï-dire ; les données factuelles, ou données objectives, seront appréciées différemment des données qui se fondent sur des appréciations ou des avis personnels, ou données subjectives.

Les données à caractère personnel collectées par la police à des fins administratives doivent être séparées logiquement et physiquement des données collectées à des fins policières. La police peut y accéder lorsque c'est nécessaire et autorisé par la loi.

Parmi les données administratives figurent, par exemple, les listes de données relatives aux titulaires de licences ou les données relatives aux ressources humaines, aux permis de port d'arme et à la perte d'un bien.

10. Communication de données au sein de la police

Il convient de faire la distinction entre la communication de données sur le plan national et le transfert international de données. Il s'agit en effet d'opérations distinctes soumises à des obligations différentes en fonction du destinataire des données : la police, un autre organe public ou un tiers privé. En général, la communication de données entre services de police ne devrait être permise que s'il existe un intérêt légitime pour cette communication dans le cadre des attributions légales de ces services.

Des règles claires et transparentes devraient définir le motif et la façon dont la police accède aux données qu'elle détient.

Les autorités policières nationales devraient ne communiquent leurs informations que lorsque la demande qui leur en est faite est prévue par la loi, par exemple en cas d'enquête judiciaire en cours ou de mission de police conjointe et dans le cadre d'une loi ou d'accords qui autorisent la communication.

La police peut communiquer des données à d'autres services de police si les données à caractère personnel sont nécessaires aux fins des enquêtes qu'ils mènent. En général, la communication de données à caractère personnel doit être soumise au principe de nécessité et de proportionnalité et servir aux fins de l'enquête.

Exemple : un service de police peut communiquer des données sur une personne soupçonnée de fraude fiscale à un autre service de police qui enquête sur une affaire de meurtre si des éléments indiquent que le suspect de ce crime pourrait être la même personne ou si cette communication pourrait matériellement aider l'enquête.

11. Communication de données par des services de police à d'autres organismes publics

La communication de données en dehors de la police est en général autorisée si cela est prévu par la loi et si ces données sont indispensables au destinataire pour accomplir la tâche licite qui lui incombe.

Des principes plus stricts devraient être respectés lorsque des données sont transmises à d'autres organismes nationaux que des services de police, car la communication pourrait servir à d'autres fins que la répression.

La communication de données à d'autres organismes publics ne devrait être autorisée que dans un cadre légal. L'entraide prévue par la loi entre services de répression et organismes publics permet à ces derniers d'avoir accès à des données policières essentielles à leurs fonctions et tâches (par exemple dans leurs enquêtes ou d'autres attributions légales conformes au droit interne).

La communication à une autre autorité publique est également autorisée si elle est effectuée dans l'intérêt certain de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent pour l'ordre public ou la sécurité publique.

Les données communiquées ne peuvent être utilisées par l'organe destinataire qu'aux fins pour lesquelles elles ont été transmises.

Exemple : demande de permis de séjour faite par un migrant. Des données policières peuvent être nécessaires pour vérifier si la personne a été impliquée dans des activités criminelles. Il serait dans l'intérêt de l'Office de l'immigration et du demandeur que cette communication de données ait lieu.

12. Communication de données par la police a des tiers privés

Il peut arriver que, dans des conditions strictes, la police ait besoin, au niveau national, de communiquer des données à des organismes privés. Cette communication doit être prévue par la loi, servir aux fins de l'enquête et être effectuée uniquement par l'autorité qui traite les données à cette fin. Elle doit faire l'objet de garanties supplémentaires telles que l'autorisation de l'organe de contrôle ou d'un magistrat, et ne devrait être effectuée qu'aux fins de l'enquête, dans l'intérêt de la personne concernée, pour des raisons humanitaires, ou s'il est nécessaire d'éviter un risque grave et imminent, pour l'ordre ou la sécurité publics.

Lorsque la police communique des données aux médias qui diffusent des informations liées à une enquête publique, il importerait d'évaluer si cela est nécessaire et dans l'intérêt public. Cette communication devrait avoir lieu au cas par cas, être chaque fois clairement prévue par la loi ou faire l'objet d'une autorisation.

Exemple : lorsque la police communique avec le secteur financier à propos de délinquants coupables de fraude ou de vol, lorsqu'elle communique avec une compagnie aérienne au sujet de documents de voyage volés ou perdus ou quand elle divulgue des informations sur une personne recherchée qui est supposée constituer un risque pour la population.

13. Transfert international

Toute communication internationale de données devrait être limitée à d'autres services de police, être adaptée au but poursuivi et prévue par la loi. Dans ce cadre, un certain nombre d'instruments juridiques internationaux multilatéraux peuvent être utiles, tels que la Convention 108 et la Constitution d'Interpol et ses documents annexes concernant le traitement des données, des cadres juridiques régionaux tels que la législation de l'UE et des institutions de l'UE (concernant Europol, Eurojust, Frontex, etc.) et des accords ultérieurs (accords bilatéraux opérationnels), des traités bilatéraux et en général des accords internationaux sur l'entraide, voire d'autres accords bilatéraux ou multilatéraux concernant la coopération et la communication.

Lorsqu'il est envisagé de communiquer des données, il conviendrait de vérifier si l'autorité destinataire a légalement une fonction qui vise la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales, et si la communication de données lui est nécessaire pour exercer ses fonctions.

L'autorité expéditrice doit veiller à ce que l'État destinataire dispose d'un niveau suffisant de protection des données et se conforme aux dispositions pertinentes en matière de communication internationale des données. Elle doit notamment prévoir des garanties adéquates en matière de protection des données au cas où il n'y aurait aucune disposition légale nationale pertinente ni aucun accord international dans ce domaine. Ce mode de transfert ne devrait être utilisé qu'en dernier ressort. Des cadres de transferts internationaux tels que le « Règlement gouvernant le traitement des données » et les « Règles sur le contrôle de l'information et l'accès aux fichiers Interpol (RCI)» , ainsi que des

dispositions de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 et de la Convention sur la cybercriminalité (STE n° 185) peuvent être très utiles pour veiller à ce que tout transfert de données soit légalement justifié t et soit encadré par des garanties suffisantes. Le demandeur doit clairement communiquer tous les éléments nécessaires pour que la partie destinataire puisse prendre une décision fondée concernant la demande, notamment le motif de celle-ci ainsi que la finalité du transfert de données.

La communication de données devrait toujours être effectuée avec un niveau de protection suffisant des données lorsqu'elle est effectuée à destination de pays qui ne sont pas parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

Si l'autorité expéditrice soumet l'utilisation des données dans l'État destinataire à un certain nombre de conditions, celles-ci devraient être respectées. Le pays expéditeur et le pays destinataire devraient être d'accord sur l'utilisation des données tout au long de leur cycle de vie.

Exemple : la retransmission à un autre destinataire des données communiquées ne devrait être autorisée que si elle est nécessaire à des fins précises identiques à celles de la communication initiale et si ce deuxième destinataire est également un service de police garantissant un niveau approprié de protection des données. Le service de police qui a envoyé initialement les données doit également donner son accord pour une éventuelle retransmission. Si un service de police du pays X envoie des données à caractère personnel à un service du pays Y, celui-ci ne peut les transférer que dans le cadre des dispositions légales susmentionnées (autrement dit si la loi encadre le transfert et si celui-ci correspond à l'objectif d'origine) et si le pays X accepte le transfert. Si les données sont communiquées à un pays Z qui n'est pas membre de la Convention 108, le pays Y doit veiller à ce que ce pays dispose d'une protection juridique adéquate en matière de traitement des données à caractère personnel et garantisse un niveau approprié de protection des données à caractère personnel.

Le transfert international de données à caractère personnel à un service qui ne dépend pas de la police n'est autorisé qu'à titre exceptionnel et dans des cas particuliers, s'il est nécessaire pour l'exécution de la tâche de l'autorité de transfert et s'il n'existe aucun autre moyen efficace de transférer les données à un service de police. Les principes de protection des données énoncés dans la Convention 108 doivent être respectés pour tous les types de transferts.

Exemple : si les autorités fiscales d'un pays X demandent à la police d'un pays Y de lui indiquer l'adresse d'une personne impliquée dans une évasion fiscale non criminelle parce qu'elle a la preuve que la personne participe à des affaires criminelles dans le pays X, la police peut transférer les données à caractère personnel de la personne concernée.

Le transfert international de données policières à des tiers privés résidant dans une juridiction différente devrait être évité en règle générale. Ce type de transfert ne peut avoir lieu que dans des cas très exceptionnels dans lesquels la gravité du crime, son caractère transfrontalier et la participation éventuelle de la police locale pourraient nuire à l'objet de l'enquête en raison de la durée de la procédure. La police locale devrait en être informée ultérieurement. La police est invitée, dans la mesure du possible, à utiliser les instruments juridiques internationaux existants en ce qui concerne ce type de transfert de données.

Exemple : dans une enquête sur du matériel pédopornographique diffusé sur internet, la victime est dans le pays Y et la police y a commencé l'enquête mais le suspect ayant mis en ligne le matériel pédopornographique réside dans un autre pays (pays X), il existe alors un risque élevé que la personne quitte le pays X. Dès lors, la police du pays Y peut demander à un fournisseur de services du pays X de lui fournir, à titre exceptionnel, des informations sur le lieu de résidence de son client. Cependant, la police du pays Y devrait informer la police du pays X de son opération le plus tôt possible et chercher à résoudre l'affaire en coopération.

14. Conditions de la communication

Le responsable du traitement a l'obligation générale de veiller à une haute qualité des données et devrait donc procéder à une vérification supplémentaire avant de communiquer des données à d'autres organismes. Toute communication ou transfert de données doit s'accompagner d'un contrôle rigoureux: de leur qualité, de leur exactitude, de leur actualité et de leur exhaustivité. Cela peut être évalué jusqu'au moment de la communication.

Exemple : les données à caractère personnel qui sont envoyées contiennent des données erronées (données à caractère personnel ou non), cela peut négativement affecter l'enquête, causer préjudice à la personne concernée ou à d'autres personnes impliquées ou qui pourraient être impliquées du fait d'un transfert de données incorrectes. Cela peut entraîner la responsabilité de l'état expéditeur comme de l'état receveur vis-à-vis des personnes concernées. L'arrestation d'une personne due à une mauvaise communication du nom du suspect porte gravement atteinte à plusieurs droits de l'homme de la personne concernée et peut affecter l'enquête criminelle.

15. Garanties concernant la communication

Il est de la plus haute importance que les principes de nécessité et de limitation de la finalité soit applicable à toute communication intérieure ou transfert international de données à caractère personnel en dehors des services de police.

Toute donnée communiquée ne devrait pas être utilisée à d'autres fins que celles pour lesquelles elle a été communiquée ou reçue. La seule exception à cela s'applique lorsque l'autorité expéditrice donne, sur une base légale, son accord pour une autre utilisation et si le traitement est prévu par la loi, est nécessaire et indispensable pour que le destinataire accomplisse sa tâche, est dans l'intérêt de la personne concernée ou pour des raisons humanitaires, ou encore est nécessaire pour prévenir un risque grave et imminent pour l'ordre public ou la sécurité publique.

Exemple : les données à caractère personnel envoyées par la police du pays X à la police du pays Y dans un cas de blanchiment d'argent ne peuvent pas être utilisées par des policiers pour mettre en place un profilage sur les croyances religieuses ou les activités politiques de la personne concernée (sauf si elles ont un lien manifeste avec le crime commis et si la police du pays X a également donné son accord pour cette utilisation).

16. Interconnexion des fichiers et accès direct (accès en ligne)

Dans des situations particulières, la police peut chercher à collecter des données en coordonnant ses informations avec celles d'autres responsables de traitement et sous-traitants. Elle peut également combiner des données à caractère personnel dans divers fichiers ou bases de données détenus à des fins différentes, par exemple des fichiers conservés par d'autres organismes publics ou privés. Ces recoupements peuvent être en relation avec une enquête criminelle en cours ou servir à repérer des tendances thématiques en relation avec un certain type de crime.

Pour être légitimes, ces démarches doivent être autorisées ou s'appuyer sur une obligation légale de se conformer au principe de limitation de la finalité.

Le service de police qui a directement accès aux fichiers d'autres services répressifs ou non répressifs ne doit y accéder et utiliser les données consultées que dans le cadre de la législation nationale qui doit prendre en compte les principes fondamentaux de la protection des données.

Il conviendrait d'élaborer une législation et des indications claires, conformes aux principes de protection des données, pour encadrer ces croisements de bases de données.

Exemple : des données conservées aux fins de la citoyenneté ne peuvent être utilisées dans une enquête que si la législation nationale le permet et dans la mesure où elles sont strictement nécessaires aux fins de l'enquête. Par exemple, le nombre d'enfants d'un suspect est une information qui n'est probablement pas utile à une enquête et ne devrait donc pas être traitée par la police.

17. Droits de la personne concernée

Le droit à l'information, le droit d'accès, le droit de rectification et le droit d'effacement sont des droits interdépendants. Le droit à l'information visé au point 4 est une condition préalable au droit d'accès ; la personne concernée a le droit d'obtenir des informations sur le traitement de ses données et d'exercer d'autres droits sur la base de ces informations. Le responsable du traitement des données doit veiller à ce que tout type de traitement des données soit notifié au public, accompagné des conditions particulières dont il est assorti (voir point 4). L'autorité de contrôle peut contribuer à la diffusion publique des informations nécessaires.

La police devrait fournir une réponse, même aux questions d'ordre général posées par les intéressés sur les activités de traitement de leurs données à caractère personnel, mais elle peut utiliser des formulaires pour faciliter la communication.

Exemple : si une personne concernée demande à la police des informations sur le traitement de ses données à caractères personnel, la police devrait répondre de façon claire, détaillée et citer des références juridiques pertinentes.

L'accès aux données est un droit fondamental reconnu à tout individu s'agissant de ses données à caractère personnel. Dans l'idéal, le droit interne devrait prévoir, en règle générale, un droit d'accès direct.

Le droit d'accès (comme le droit à l'information) devrait, en principe, être gratuit. La police peut refuser de répondre aux demandes manifestement infondées ou excessives, notamment lorsque leur caractère répétitif justifie un tel refus.

Il est possible de facturer des frais administratifs raisonnables pour la demande si la législation nationale le prévoit.

Pour que l'exercice du droit d'accès soit équitable, la communication « sous une forme intelligible » s'applique aussi bien au contenu qu'à la forme d'une communication numérique standardisée.

S'il s'agit d'un accès direct, la personne concernée peut demander au responsable du traitement un accès aux fichiers. Le responsable du traitement des données évaluera la demande et toute restriction éventuelle qui ne peut être appliquée que dans la mesure où elle serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui. Il répondra directement à la personne concernée.

S'il s'agit d'un accès indirect, la personne concernée peut adresser sa demande à l'autorité de contrôle qui traitera la demande en son nom et procédera à des vérifications sur la disponibilité et la légalité de ses données à caractère personnel. L'autorité de contrôle répondra ensuite à la personne concernée (à condition que les données puissent être diffusées, sous réserve des restrictions autorisées légalement).

Le responsable du traitement des données devrait évaluer la demande et répondre à la personne concernée dans le délai raisonnable prévu par le droit interne.

Il faudrait que les dispositions en vigueur prévoient le moyen de confirmer l'identité de la personne concernée avant toute autorisation d'accès à des données et de même s'il délègue à un tiers la faculté d'exercer ses droits.

Exemple : la demande d'accès peut être refusée si une enquête est en cours sur la personne concernée et que l'octroi d'un accès lui permette de compromettre l'enquête. Toutefois, il est conseillé de se référer à la législation nationale pour veiller à ce que la réponse soit cohérente, et pour éviter que des suspects utilisent cette méthode pour savoir s'ils font l'objet d'une enquête en cours.

Le droit d'une personne concernée de pouvoir modifier toute donnée inexacte détenue à son sujet est un droit essentiel. La personne concernée qui découvre des données inexactes, excessives ou non pertinentes devrait avoir le droit de les contester et de veiller à ce qu'elles soient modifiées ou supprimées.

Dans certains cas, il peut être utile d'ajouter au fichier des informations supplémentaires ou rectificatives. Si les données à corriger ou à effacer ont été communiquées à des tiers, il appartient aux autorités compétentes d'informer ces derniers des modifications à apporter.

Toutes les modifications proposées devraient être étayées par des éléments de preuve. Si les personnes concernées peuvent prouver au moyen de documents officiels du même pays que les données traitées par la police à leur égard sont incorrectes, le responsable du traitement n'aura pas la liberté de décider s'il faut les rectifier ou les supprimer.

La police peut avoir besoin de ne pas donner d'informations ou de ne pas accorder un droit d'accès qui pourrait compromettre une enquête (voir le point 5). La divulgation de ces données devrait donc être exclue pendant toute la durée de l'enquête.

Les restrictions imposées à la communication de données ne devraient s'appliquer que dans la mesure où elles sont nécessaires et faire l'objet d'une interprétation restreinte. Chaque demande de la part des personnes concernées devrait être évaluée soigneusement, au cas par cas.

Tout refus de donner suite à une demande d'une personne concernée devrait être communiqué par écrit (y compris par des moyens électroniques) et indiquer clairement les motifs de la décision qui pourront être vérifiés par une autorité indépendante ou un juge.

Il peut arriver que le fait de communiquer les motifs d'un refus présente un risque pour la police, la personne concernée ou les droits et libertés d'autrui. En pareil cas, il importe que le refus soit transmis, documents à l'appui, à l'autorité indépendante ou au juge qui vérifiera si nécessaire son bien-fondé.

La personne concernée peut être amenée, selon la législation nationale, à fournir un extrait de son casier judiciaire. Or la fourniture d'une copie ou d'une communication écrite n'est peut-être pas dans son intérêt; dans ce cas, le droit interne peut autoriser la communication orale du contenu demandé.

Exemple : si une personne A a fait une déclaration au sujet d'une personne B l'accusant d'avoir commis une grave infraction et qu'il s'avère par la suite que cette accusation était fausse, les services de police peuvent juger utile de conserver cette fausse déclaration et les informations qu'elle comprenait.

Au lieu de supprimer la déclaration dont la fausseté a été démontrée, ils peuvent ajouter au fichier concerné une déclaration rectificative claire.

Il convient d'informer la personne concernée de toutes les possibilités dont il dispose en cas de refus, comme le dépôt d'un recours auprès de l'autorité de contrôle ou d'une autre autorité administrative indépendante.

Exemple : une lettre de refus envoyée par la police doit contenir le nom, l'adresse, l'adresse internet, etc. de toutes les instances de recours possibles.

À chaque fois qu'elle n'est pas satisfaite d'une réponse donnée par l'autorité de contrôle ou par l'autorité indépendante, la personne concernée devrait avoir la possibilité de saisir une cour ou un tribunal afin de contester la décision et de faire examiner les motifs du refus. L'autorité de contrôle devrait disposer de pouvoirs suffisants pour examiner le fichier de police concerné et pour recevoir l'appréciation de la demande d'accès.

L'issue de cet examen ou du recours peut varier en fonction de la législation nationale et de l'existence d'un droit d'accès direct ou indirect. Il peut arriver que l'autorité de contrôle ne soit pas toujours obligée de communiquer les données à la personne concernée, même si rien ne s'oppose à ce qu'elle puisse y accéder. Dans ce cas, la personne concernée devrait être informée du fait que le fichier de police a fait l'objet d'une vérification. À défaut, l'autorité de contrôle peut décider de communiquer les données du fichier à la personne concernée. En outre, la juridiction compétente peut avoir le pouvoir d'ordonner l'accès aux données du fichier, leur rectification ou leur suppression.

18. Sécurité des données

La police doit prendre des mesures adéquates de sécurité pour lutter contre des risques tels que l'accès accidentel ou non autorisé à des données à caractère personnel ou la destruction, la perte, l'utilisation, la modification ou la divulgation de ces données. Le responsable du traitement doit, au minimum, informer sans délai l'autorité de contrôle compétente de ces violations de données qui peuvent gravement porter atteinte aux droits et libertés fondamentales des personnes concernées.

La sécurité des informations est essentielle à la protection des données. Il s'agit d'un ensemble de procédures destinées à garantir l'intégrité de toutes les formes d'information et qui doit être mis en place au sein de la police en vue d'assurer la sécurité des données et des informations et de limiter l'incidence des incidents de sécurité à un niveau prédéterminé.

Le niveau de protection conférée à une base de données et/ou à un système ou un réseau informatique est déterminé au moyen d'une évaluation des risques. Plus les données sont sensibles, plus la protection devra être importante.

Les mécanismes d'autorisation et d'authentification sont essentiels à la protection des données et il conviendrait de procéder au chiffrement systématique des informations sensibles. La mise en place d'un dispositif régulier de vérification de l'adéquation du niveau de sécurité est considérée comme une bonne pratique.

Il est conseillé aux services de police de procéder à une évaluation de l'impact sur le respect de la vie privée de la personne concernée s'agissant de la collecte, de l'utilisation et de la divulgation des informations. Elle permettra de recenser les risques et d'élaborer des solutions pour remédier efficacement aux défaillances constatées.

Un délègue à la protection des données (DPD) au sein de police peut jouer un rôle essentiel dans la réalisation de vérifications internes et l'évaluation de la légalité du traitement. Cette fonction contribue au renforcement de la protection de la sécurité des données. En outre, ce délègue peut faciliter le dialogue entre l'administration et les personnes concernées et entre l'administration et l'autorité de contrôle, ce qui peut également renforcer la transparence globale du service de police.

Il est recommandé d'utiliser un Système de gestion de 'identité et des accès pour gérer l'accès des employés et des tiers aux informations. L'accès au système sera soumis à une authentification et à une autorisation ; un système de droits réservés permettra de déterminer les données consultables. Un tel système est essentiel pour garantir un accès sécurisé et adéquat aux données.

Le responsable du traitement des données met en œuvre, après une évaluation des risques, les mesures destinées à garantir :

- le contrôle de l'accès à l'équipement,
- le contrôle des supports des données,
- le contrôle de l'enregistrement des données,
- le contrôle des utilisateurs,
- le contrôle de l'accès aux données,
- le contrôle de la communication des données,
- le contrôle de la saisie des données,
- le contrôle du transfert des données,
- la récupération des données et l'intégrité du système,
- la fiabilité et l'intégrité des données.

Le respect de la vie privée dès la conception

La vie privée fait partie intégrante de la sécurité. La protection et la sécurité des données peuvent être directement intégrées dans les systèmes et processus d'information afin d'assurer un niveau élevé de protection et de sécurité des données et, en particulier, de réduire au minimum le risque de violation des fichiers. Cette approche, appelle respect de la vie privée dès la conception, favorise dès le début la protection de la vie privée et des données. Elle peut être mise en place au moyen d'un logiciel et/ou d'un matériel informatique. Elle suppose une analyse des risques, une approche fondée sur un cycle de vie complet et une vérification rigoureuse.

Il importe que les responsables du traitement veillent à ce que la protection de la vie privée et des données soit rigoureusement prise en compte aux premiers stades d'un projet, puis tout au long de son cycle de vie. C'est tout particulièrement le cas lorsqu'on conçoit un nouveau système informatique d'enregistrement de données à caractère personnel ou d'accès à celles-ci, lorsqu'on élabore une législation, une politique ou une stratégie ayant des répercussions sur la vie privée et lorsqu'on met en place un partage des informations qui utilise des données à de nouvelles fins.

Les technologies de renforcement de la protection de la vie privée (PET)

Ce terme désigne un éventail de technologies différentes qui visent à protéger les données à caractère personnel sensibles dans les systèmes informatiques. Le respect de la vie privée dès la conception suppose la mise en œuvre de technologies de renforcement de la protection de la vie privée qui permettent aux utilisateurs de mieux protéger leurs données à caractère personnel. Ces technologies empêchent le traitement excessif des données à caractère personnel sans réduire les capacités fonctionnelles du système informatique.

Elles sont principalement utilisées pour déterminer si des informations identifiables sont nécessaires à l'élaboration ou la conception d'un nouveau système informatique, ou à l'amélioration d'un système existant.

Exemple : les scanners corporels utilisés à des fins policières doivent être conçus pour respecter la vie privée des individus à inspecter tout en répondant à l'objectif de leur utilisation. C'est pourquoi l'image du corps qui apparaît dans ces outils doit être brouillée par défaut.

19. Contrôle externe

Au minimum, une autorité de contrôle doit être chargée de veiller à la conformité du traitement des données avec la législation nationale et internationale dans le secteur de la police.

Certains États membres peuvent exiger l'existence de plusieurs autorités de contrôle, par exemple une autorité nationale ou fédérale et plusieurs d'autorités décentralisées ou régionales, tandis que d'autres préféreront une seule autorité de contrôle, responsable de l'intégralité de la supervision des opérations de traitement des données à caractère personnel.

L'organe de contrôle devrait être totalement indépendant et donc ne pas appartenir à un service de répression ou à l'exécutif d'une administration nationale. Il devrait disposer des ressources suffisantes pour exécuter ses tâches et fonctions.

La législation nationale doit conférer à cet organe des pouvoirs d'enquête et des pouvoirs répressifs lui permettant de mener une enquête à la suite d'une plainte, d'appliquer des mesures réglementaires ou d'infliger des sanctions par le cas échéant.

Les autorités de contrôle devraient avoir la capacité de coopérer bilatéralement dans le domaine répressif et par l'intermédiaire du Comité de la Convention 108.

Exemple : l'autorité de contrôle doit être instituée en dehors du pouvoir exécutif et disposer de tous les pouvoirs nécessaires pour accomplir sa tâche. Une autorité mise en place au sein d'un ministère ou de la police elle-même ne remplit pas cette obligation.

Glossaire/définitions

Aux fins du présent guide :

a. « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (« la personne concernée ») ;

b. « données génétiques » : toutes les données concernant les caractéristiques génétiques d'une personne qui ont été héritées ou acquises durant la phase de développement prénatal, tels qu'elles résultent d'une analyse d'un échantillon biologique de la personne concernée : analyse chromosomique, analyse d'ADN ou d'ARN ou analyse de tout autre élément permettant d'obtenir des informations équivalentes ;

c. « données biométriques » : données résultant d'un traitement technique spécifique des données concernant les caractéristiques physiques, biologiques ou physiologiques d'une personne et qui permettent son identification ou son authentification ;

d. « donnés subjectives » : données acquises par le biais de témoignages de personnes impliquées dans l'enquête ;

e. « données objectives » : données acquises provenant de documents officiels ou d'autres sources certifiées ;

f. « traitement de données » : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données. Lorsqu'un traitement automatisé n'est pas utilisé, le traitement de données désigne une opération ou un ensemble d'opérations effectuées sur des données à caractère personnel présentes dans un ensemble structuré de ces données qui sont accessibles ou récupérables selon des critères spécifiques ;

g. « autorité compétente » : organisme public ou privé habilité par la loi et disposant d'une compétence dans la prévention, les enquêtes, les poursuites des infractions pénales et l'exécution des sanctions pénales ;

h. «responsable du traitement » : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données;

i. « destinataire » :la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles;

j. «sous-traitant»: la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. ;

k. « Internet des objets » (Internet stylisé des objets ou IdO) : interconnexion d'appareils physiques, de véhicules (également appelés « appareils connectés » et « appareils intelligents »), de bâtiments et d'autres dispositifs intégrant de l'électronique, des logiciels, des capteurs, des actionneurs ; et connectivité réseau qui permettent à ces objets de collecter et d'échanger des données ;

l. « surveillance discrète » : toutes les mesures visant à surveiller discrètement les mouvements de personnes, de véhicules et de conteneurs, en particulier ceux qui sont employés par la criminalité organisée ou transfrontière.

m. « techniques d'enquêtes spéciales » : techniques appliquées par des autorités compétentes dans le contexte d'enquêtes criminelles en vue de détecter des crimes graves et d'identifier des suspects et

d’enquêter sur eux dans le but de rassembler des informations de telle manière à ne pas attirer l’attention de la personne visée.