COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 17 novembre 2017 T-PD(2016)02rev11

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 dans le secteur de la police

Version révisée préparée par le Secrétariat suite aux commentaires reçus

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 dans le secteur de la police énonce un ensemble général de principes à appliquer dans ce secteur pour garantir le respect du droit à la vie privée et à la protection des données 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 son application que de sa pertinence. En 2010, le Comité consultatif de la Convention 108 a décidé de réaliser une étude[1] sur l'utilisation de données à caractère personnel dans le secteur de la police dans l'ensemble de l'Europe. Cette évaluation a montré que les principes de la Recommandation (87)15 constituaient toujours un point de départ approprié pour élaborer des réglementations s'appliquant à cette matière au niveau national et que l'élaboration d'un guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police, sur la base des principes énoncés par la Recommandation (87)15, fournirait des éléments d'orientation sur ce que ces principes impliquent au niveau opérationnel.

Le présent guide a donc été élaboré pour mettre en évidence les questions les plus importantes qui peuvent se poser dans le cadre de l'utilisation de données à caractère personnel par la police et pour signaler les principaux éléments à prendre en compte dans ce contexte.

Il ne reproduit ni les dispositions de la Convention 108 ni celles de la Recommandation (87)15 mais se concentre sur des éléments d'orientation pratiques.

Les principes généraux de la Recommandation (87)15 et leurs implications pratiques visent à ce que, lors de l'utilisation des données personnelles par la police, un juste équilibre soit établi entre les objectifs essentiels de l'intérêt public général (prévention, investigation et poursuite des infractions pénales, exécution des sanctions pénales et maintien de l'ordre public) et le respect des droits des individus à la vie privée et à la protection des données.

Il convient de souligner que le Guide vise à donner des orientations sur des situations pratiques auxquelles la police est confrontée dans son fonctionnement quotidien et reconnaît que la collecte et l'utilisation légitimes de données personnelles à des fins de respect de la loi sont cruciales pour la sécurité nationale et pour la prévention des crimes ou le maintien de l'ordre public. Il démontre avec des exemples concrets que la prévention et la répression de la criminalité, y compris par le biais de la collecte et de l'utilisation de données personnelles afin de faire respecter la loi, peuvent être menées efficacement en conformité avec la loi.

Pour faciliter la lecture du 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.

Considérations générales

La collecte et l'utilisation de données à caractère personnel à des fins policières constitue une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel prévu par l'article 8 de la Convention européenne des droits de l'homme et par la Convention 108 et doivent par conséquent être fondés 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.

Tout traitement de données doit être entièrement conforme aux principes de nécessité, de proportionnalité et de limitation de la finalité. Cela signifie que le traitement de données personnelles par la police devrait être effectué sur la base d'un but prédéfini, précis et légitime prévu par la loi. Il devrait être nécessaire et proportionné à ces fins légitimes et en aucun cas effectué d'une manière qui soit incompatible avec ces finalités. En outre, ce traitement devrait être assuré de façon licite, loyale et transparente, et être adéquat, pertinent et non excessif par rapport aux finalités. Enfin, les données 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, c'est-à-dire à des fins de prévention, d'investigation et de répression des infractions pénales, d'exécution des sanctions pénales [et du maintien de l'ordre public par la police] (désignée plus loin par : « les tâches de la police », [« les finalités policières »]). Le terme « police » utilisé dans le texte désigne plus généralement les services chargés de l'application de la loi, notamment les services du procureur général 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

La police en tant que responsable du traitement de données, assume toutes les responsabilités concernant les traitements qu'elle effectue et sur lesquels elle doit rendre des comptes.

La collecte de données personnelles pour des objectifs de police devrait être limitée à ce qui est nécessaire et proportionné à la prévention d'un danger réel ou la suppression d'une infraction précise. Toute exception à cette disposition devrait faire l'objet d'une législation nationale particulière.

Il est compris par le point 2.1 de la Recommandation que, dans l'accomplissement des deux tâches principales de la police (prévention d'un danger réel et suppression d'une infraction précise), une corrélation évidente et directe doit exister entre le traitement des données effectué par la police et une situation où des individus ont commis ou sont susceptibles de commettre un crime.

La police devrait toujours choisir la base légale appropriée pour traiter des données personnelles et le faire de façon légitime. Elle devrait soigneusement évaluer si le traitement a bien une base légale et si les procédures prévues sont entièrement respectées.

La police devrait appliquer les principes de la protection des données pertinents à tous les stades du traitement (surtout les principes de nécessité, proportionnalité et limitation de finalité) et ne devrait pas traiter des données qui ne sont plus nécessaires au but poursuivi. Dans ce contexte, les données personnelles collectées à une phase précoce d'une enquête et qui au long de l'enquête se révèlent n'être plus pertinentes ne devraient plus être traitées (par exemple, quand l'innocence d'un suspect est confirmée). Elles devraient donc être bloquées ou supprimées. Cela ne s'applique pas lorsqu'une utilisation ultérieure des données est autorisée (point 3).

Une utilisation ultérieure des données est considérée comme une nouvelle opération de traitement qui doit remplir tous les critères et les conditions mentionnés plus haut. L'utilisation ultérieure des données doit être licite, servir une finalité légitime et y être nécessaire et proportionnée.

Avant et pendant la collecte de données à caractère personnel, il faudrait toujours se demander si de telles données collectées sont nécessaires à l'enquête ou à d'autres tâches de la police comme décrites au point 1. Il convient de noter que, une fois les données personnelles recueillies, il devrait

exister un lien clair entre la personne dont les données sont traitées et le but du traitement (c'est-à-dire l'enquête ou la tâches spécifiques de la police). Ce lien, ainsi que la conformité aux principes de protection des données décrites dans ce Guide, doivent être démontrés à tout moment. Après la collecte et aux différents stades de l'enquête et de la poursuite, il faut impérativement procéder à une analyse approfondie pour évaluer quelles sont les données qui doivent être conservées et celles qui doivent être effacées.

Selon le principe de responsabilité, la police, comme tout autre responsable du traitement, est responsable du traitement des données qu'elle entreprend. Cela implique qu'elle doit être en mesure de démontrer à tout moment que ses activités de traitement sont conformes aux règles de la protection des données. En outre, il exige que la police prenne activement des mesures pour sauvegarder et promouvoir la protection des données dans toutes ses activités.

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

Exemple : S'agissant de données personnelles telles que des factures téléphoniques, seuls le(s) numéro(s) nécessaire(s) à la période sur laquelle porte l'enquête devraient être demandés et uniquement pour la ou les personnes susceptibles d'être en lien avec l'infraction.

Une liste des numéros de téléphone de la ou des personnes impliquée(s) dans l'infraction présumée peut être obtenue si des éléments existent indiquant que ces données peuvent servir l'enquête. Elles ne peuvent pas être conservées ou traitées une fois que l'analyse a montré qu'elles n'étaient pas strictement nécessaires à la finalité de l'enquête.

Le classement et le traitement 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.

Conformément au principe de limitation de la finalité, les données à caractère personnel collectées à des fins policières doivent servir exclusivement à ces fins et ne doivent pas être utilisées à des fins incompatibles avec la finalité initiale énoncée au moment de la collecte, sauf disposition contraire de la loi (voir article 9 de la Convention 108). [Lors de l'évaluation de la compatibilité de l'utilisation des données pour une même finalité, les critères suivants devraient être pris en compte : (i) relation entre les objectifs ; (ii) contexte de la collecte et informations fournies aux personnes concernées ; (iii) nature des données personnelles ; (iv) conséquences pour les personnes concernées de l'utilisation ultérieure envisagée ; (v) existence de garanties appropriées.]

Comme cela est indiqué dans les Considérations générales la police devrait s'assurer, à toutes les étapes du traitement des données et pour leur utilisation ultérieure, que les données personnelles sont exactes, à jour, adéquates, pertinentes et non excessives par rapport aux buts pour lesquels elles sont traitées.

Exemple : Des données collectées par la police dans le cadre d'une enquête où l'affiliation politique de la personne concernée n'a pas d'importance ne peuvent pas être utilisées pour déterminer l'appartenance politique de la personne concernée, sauf si la loi l'autorise.

3. Utilisation ultérieure des données

Tout traitement ultérieur de données pour des finalités policières autres que celles pour lesquelles elles ont été recueillies en premier lieu, doit respecter les obligations légales applicables au traitement de données à caractère personnel : être prévu par la loi, poursuivre une finalité légitime et être nécessaire et proportionné au but légitime poursuivi.

Les données à caractère personnel traitées ultérieurement devraient avoir un lien avec une finalité policière et doivent satisfaire aux mêmes critères et conditions qu'énoncés pour la collecte et

l'utilisation des données au point 2. La règle générale est que si les données sont susceptibles d'être utilisées dans un autre dossier ou dans une autre opération de police, l'analyse de conformité décrite au point 2 devrait être appliquée également pour le nouveau traitement. (Cela n'est pas applicable si les données sont utilisées dans un but purement statistique ou scientifique). Nonobstant le traitement numérique et / ou automatisé des données et du volume important de données personnelles stockées très souvent dans des environnements de traitement différents, les données personnelles recueillies et conservées à des fins de police ne doivent pas être conservées et traitées à des fins non spécifiques ou générales ou d'une manière incompatible au principe de limitation de finalité.

Il convient par ailleurs de noter que toute utilisation ultérieure de données à caractère personnel liées à des personnes vulnérables telles que victimes, mineurs, personnes bénéficiant d'une protection internationale, devrait faire l'objet d'une attention particulière et devrait être soumise à une analyse juridique qui veillerait particulièrement à l'application des principes de nécessité et de proportionnalité.

Dans des affaires comme celles concernant la traite d'êtres humains, le trafic de drogue, l'exploitation sexuelle, etc., ou dans lesquelles les données des victimes peuvent être utilisées ultérieurement lorsqu'elles sont aussi considérées comme des suspects, ou dans lesquelles 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 d'améliorer la façon dont ils échangent des informations sur la question au sein des organismes régionaux ou internationaux.. Si toutes les exigences légales telles qu'énoncées au point 2 sont remplies, cela ne devrait pas présenter d'obstacle à l'utilisation des données de ces personnes à des fins de police, mais les règles de confidentialité doivent être respectées pendant ces échanges.

Exemple - Les données rassemblées à des fins fiscales auprès d'une personne concernée ne peuvent être traitées pour des fins de police que si la loi l'autorise, si elles sont utilisées dans un but légitime et d'une manière nécessaire et proportionnée au but recherché. Dans le cadre concret d'une enquête sur le blanchiment d'argent, l'utilisation des données de déclarations fiscales d'un particulier peut être envisagée pour établir ou nier un lien entre l'individu et les opérations de blanchiment d'argent.

4. Traitement portant sur des catégories particulières de données (données sensibles)

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 de façon unique une personne, des données personnelles 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 la loi l'autorise et que des garanties appropriées ont été mises en place pour palier des risques potentiels de discrimination ou d'impact juridique défavorables affectant de manière significative les personnes concernées. Les garanties peuvent être de nature technique, par exemple des mesures de sécurité supplémentaires, et de nature organisationnelle, par exemple, en traitant les données sensibles séparément de l'environnement de traitement des catégories de données "ordinaires". Les sauvegardes devraient être ajustées à chaque opération de traitement de données en tenant compte de leurs spécificités et il est fortement recommandé d'utiliser plusieurs niveaux de protection pour ces catégories de données (par exemple : trames principales séparées, périodes de conservation de données plus courtes, etc.). Il est primordial d'empêcher un accès non autorisé ou indésirable à ces catégories de données, même avec des mesures de sécurité additionnelles.

Un équilibre soigneux des intérêts prenant en compte le but de l'enquête, le contexte et la nature des données est nécessaire pour déterminer si oui ou non et dans quelle mesure la police pourrait traiter des données sensibles. Par exemple, lorsque les données biométriques sont traitées par la police, il serait conseillé de différencier, si c'est dans un but d'identification (quand par exemple, deux empreintes digitales pourraient suffire) ou pour une enquête criminelle (où d'avantages d'empreintes digitales pourraient être nécessaires).

La mise en œuvre d'évaluations d'impact de la protection des données (DPIA) est recommandée afin de s'assurer que les garanties appropriées sont mises en place. Elle est généralement effectuée quand le type de traitement appliqué peut entrainer un risque important pour les droits et les libertés des personnes. Le responsable du traitement devrait évaluer et démontrer si le but du traitement peut être réalisé d'une manière qui ait le moins d'impact sur le droit à la vie privée et la protection des

données et si le traitement de catégories spéciales de données ne représente pas un risque de discrimination pour la personne.

De plus, il convient de rappeler que la collecte et le traitement de données sensibles dans le contexte du profilage sont interdits (Principe 3.11 de la Recommandation 2010(13))[2] sauf si ces données sont nécessaires et proportionnées aux finalités légitimes et spécifiques du traitement et pour autant que le droit interne prévoit des garanties appropriées. Dans ce contexte, en plus des mesures détaillées ci-dessus, on peut recommander l'utilisation de technologies de renforcement de la protection de la vie privée (PET) et de contrôles plus fréquents sur la légalité du traitement. Cela pourrait, par exemple, se traduire par des mesures mises en place pour contrer l'hypothèse que les individus appartiennent à une organisation criminelle en raison de leur lieu de résidence où une organisation criminelle est active ou où les personnes ont une même origine ethnique.

Exemple : Cibler des groupes ou des individus seulement sur la base de motifs 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 (liées au lieu de culte, aux prédicateurs religieux, aux coutumes, à l'enseignement, aux membres et à la structure de la communauté religieuse, etc.) et qui sont pertinents pour l'enquête.

5. 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 doit communiquer au public des *informations générales* sur le traitement des données qu'il effectue et 2) il doit donner aux intéressés des informations *spécifiques* sur le traitement de leurs données à caractère personnel si aucune des restrictions ou dérogations décrites au point 7 ne s'applique à cet égard.

Les informations données au public dans son ensemble devraient permettre de le sensibiliser, de l'informer de ses droits et d'offrir des orientations claires concernant les modalités de leur exercice. Les informations fournies devraient être largement et effectivement accessibles. Par ailleurs, elles devraient également préciser dans quelles conditions les droits des intéressés peuvent faire l'objet d'exceptions et comment ils pourraient former un recours devant l'autorité de contrôle ou un tribunal.

Les sites internet et autres média facilement accessibles jouent un rôle dans l'information du public. Il est recommandé de mettre des lettres-types à la disposition des personnes concernées qui souhaitent exercer leurs droits. Il est de la responsabilité du responsable du traitement de fournir une information qui met en lumière la protection des données et les droits des personnes concernées.

Afin de respecter la deuxième obligation de fournir aux personnes concernées des informations spécifiques concernant les données traitées, la police doit les informer sur le traitement des données envisagé avant le traitement ou après si cela n'est pas possible pour des raisons objectives. Cette communication comprendra des informations sur le traitement des données, la collecte des données des personnes et des renseignements complets sur leurs droits. L'obligation de fournir des informations spécifiques implique que, en principe, les personnes concernées reçoivent des détails tels que le nom et les coordonnées du responsable du traitement de données, le sous-traitant des données, les destinataires, l'ensemble de données à traiter, le but de leur traitement, la base juridique pour le faire et des informations sur leurs droits.

Les informations doivent être fournies à moins qu'une restriction ou une dérogation ne s'applique comme décrit au point 7, en tenant compte de la spécificité des fichiers de police, tels que les fichiers de renseignements criminels, les fichiers contenant d'autres types de données sensibles. Afin d'éviter

[2] Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

de nuire gravement à l'exercice des fonctions de la police, y compris des services des procureurs généraux, ou aux droits des individus, même si des restrictions ou des dérogations au droit à l'information étaient appliquées, des informations devraient être fournies aux personnes concernées dès que cela ne créé plus d'obstacle au but pour lequel leurs données ont été utilisées.

Très souvent les personnes concernées ne peuvent pas recevoir des informations complètes sur le traitement que la police entreprend sur leurs données en raison de restrictions ou de dérogations à leur droit à l'information ; cela ne devrait pas affecter leur exercice du droit d'accès.

Exemple : Pour procéder à la surveillance discrète d'un délinquant sexuel à haut risque, il peut être justifié de ne pas informer l'intéressé sous surveillance du traitement de ses données et de leur conservation prolongée si l'on considère que cela peut nuire à l'enquête en cours ou planifiée. Cependant, une fois que le but de la surveillance secrète est atteint et si aucune des restrictions ou des dérogations n'est applicable, la personne concernée doit être informée qu'elle ou il a été sujet(te) à une telle mesure.

6. Droits de la personne concernée

L'accès à ses données est un droit fondamental reconnu à tout individu car cela lui permet d'être au courant des traitements qui sont effectués sur des données qui le concernent. De plus, cela peut constituer un prérequis pour l'exercice d'autres droits comme le droit d'être informé, le droit à la rectification et le droit à la suppression.

La police [en principe] doit informer les personnes sur les traitements des données qui les concernent. Dans le cas où la police collecte des données d'un individu au cours d'une enquête ou pour d'autres tâches policières décrites au point 1, dès que les circonstances l'autorisent en toute sécurité, elle devrait en principe l'informer du traitement des données s'il le demande. L'information devrait être fournie sur demande. La communication doit contenir les mêmes informations que celles décrites au point 5, à moins que les personnes concernées ne le souhaitent autrement.

La loi peut prévoir, dans les conditions strictes décrites au point 7, que le droit d'accès puisse également être limité ou exclu si cela porte préjudice à l'enquête ou à d'autres tâches importantes de la police, aux intérêts de l'État (comme la sécurité publique, la sécurité nationale, etc.) ou à la protection des droits et libertés d'autrui. Cependant, le fait de ne pas donner d'informations sur le traitement des données par la police devrait être une exception et pouvoir être clairement justifié.

La police devrait chercher à répondre 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 par email, s'il n'y a pas d'exception applicable et après vérification de l'identité de la personne concernée, la police devrait apporter une réponse détaillée en indiquant les références juridiques pertinentes, comprenant la liste des dossiers dans lesquels les données de la personne concernée sont traitées, et ce de façon claire, détaillée, sans utiliser d'expressions peu courantes ou spécialisées.

En principe, le droit d'accès devrait être gratuit.

Il est possible de facturer des frais administratifs raisonnables pour la demande si la législation nationale le prévoit et si la demande est manifestement infondée ou excessive. La police peut également refuser de répondre à de telles demandes manifestement infondées ou excessives, en particulier lorsque leur caractère répétitif le justifie.

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. Il est toutefois recommandé de se référer à la législation nationale pour assurer une cohérence et éviter que des suspects utilisent cette méthode pour découvrir s'ils font l'objet d'une enquête.

S'il s'agit d'un accès direct, la personne concernée peut demander un accès au responsable du traitement. Après avoir évalué la demande et l'application de toute restriction ou dérogation éventuelle qui ne pourrait être appliquée que dans la mesure où elle serait indispensable pour l'accomplissement d'une tâche légale de la police comme prévu au point 1, ou serait nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui, le responsable du traitement répond directement à la personne concernée. Dans le cas d'une restriction ou d'une information partielle et dans le cas d'une dérogation, la personne concernée doit tout de même recevoir une information sur l'application de ces mesures assortie des motifs qui les justifient, ainsi qu'une information sur ses voies de recours.

Exemple : La demande d'accès peut être refusée si une enquête est en cours sur la personne concernée et si lui permettre d'accéder aux données risque de la compromettre.

Si une restriction ou une dérogation devait être utilisée, toute réponse devrait tenir compte, conformément à la législation ou à la pratique nationale, de toutes les circonstances pour lesquelles la restriction ou la dérogation est applicable.

En règle générale, le droit interne devrait idéalement prévoir un accès direct. Si le droit d'accès prévu est indirect, la personne concernée peut adresser sa demande à l'autorité de contrôle qui, après avoir été dûment mandatée, la traitera en son nom et procédera à des vérifications sur la disponibilité et la licéité du traitement des données à caractère personnel. L'autorité de contrôle répondra ensuite à la personne concernée (en fonction des données qu'il est possible de diffuser, sous réserve des restrictions ou dérogations autorisées légalement). Dans le cas d'une restriction ou d'une dérogation, la même communication que celle applicable à l'accès direct devrait être rendue possible.

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

Les dispositions en vigueur devraient prévoir le moyen de confirmer l'identité de la personne concernée et d'obtenir des informations sur les activités de traitement auxquelles la demande se réfère avant toute autorisation d'accès aux données. Il doit en être de même si la personne concernée délègue à un tiers la faculté d'exercer ses droits.

Le droit d'une personne concernée de pouvoir modifier toute donnée inexacte détenue à son sujet ou à demander l'effacement des données qui ne s'avèrent pas pertinentes ou dont le traitement est excessif, ou autrement illicite est un droit essentiel. Une personne concernée qui découvre des données inexactes ou non pertinentes devrait avoir le droit de les contester et de veiller à ce qu'elles soient rectifiées ou supprimées.

Dans certains cas, il peut être utile d'ajouter au fichier des informations supplémentaires ou rectificatives. Il est important de souligner que ce droit peut seulement être exercé dans le respect des droits d'autrui.

Si les données à corriger ou à effacer ont été communiquées à des tiers, ces derniers doivent être informés 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 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.

Conformément à ce qui est prévu au point 7, la police peut avoir besoin de ne pas donner d'informations ou de droit d'accès, de suppression ou de correction qui pourrait compromettre une enquête. La divulgation de ces données devrait donc être exclue pendant toute la durée de l'enquête. Des restrictions ou des dérogations similaires peuvent être prescrites par la loi nationale comme décrit au point 7.

Les restrictions ou dérogations imposées aux droits de la personne concernée 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 de personnes concernées devrait être évaluée soigneusement, au cas par cas. Tout refus de donner suite à la demande d'une personne concernée devrait être communiqué

par écrit (y compris par des moyens électroniques). La réponse devrait indiquer clairement les motifs de la décision qui pourraient 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, pour la personne concernée ou pour 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.

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 sa déclaration contenant cette accusation était fausse, les services de police peuvent juger utile de conserver cette fausse déclaration et les informations qu'elle comprenait, même si la personne concernée demande sa suppression au motif que les données traitées ne sont pas correctes.

Bien que la déclaration se soit avérée fausse, si la police a besoin de conserver des données dans l'intérêt d'une enquête par exemple, une déclaration corrective claire serait nécessaire dans le dossier au lieu de supprimer la fausse déclaration.

Il convient d'informer la personne concernée de toutes les possibilités dont elle dispose en cas de refus, comme le dépôt d'un recours auprès de l'autorité de contrôle, d'un tribunal ou d'une autre autorité administrative indépendante. La communication effective de 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. Dans le cas d'un accès indirect, la personne concernée devrait au moins être informée du fait que le fichier de police a fait l'objet d'une vérification. À défaut, l'autorité de contrôle peut demander à la police de communiquer les données du fichier à la personne concernée. Une cour ou un tribunal peut avoir le pouvoir d'ordonner l'accès aux données du fichier, leur rectification ou leur suppression, même dans le cas où une demande d'accès lui a été transmise par la police ou l'autorité de contrôle.

Une lettre de refus envoyée par la police doit contenir le nom, l'adresse, l'adresse internet, etc. de toutes les formes de recours possibles.

Si 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.

7. Exceptions à l'application des principes de protection des données

Conformément à l'article 8 de la Convention européenne des droits de l'homme et à la Convention 108, les exceptions ne peuvent être utilisées que si elles sont prévues par la loi (celle-ci doit être publique, ouverte, transparente ainsi que suffisamment détaillée), si elles constituent une mesure nécessaire et proportionnée dans une société démocratique et si elles sont utilisées 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, la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres objectifs essentiels d'intérêt général (ce qui inclut des objectifs liés au respect d'engagements ou d'obligations internationaux de l'État, principalement découlant de décisions contraignantes d'organes des Nations Unies ou d'objectifs humanitaires) ou la protection des droits et libertés fondamentales d'autrui.

Les exceptions qui doivent être intégrées au droit national ne devraient pas être décrites en général mais répondre à un objectif clairement défini. Des exceptions peuvent être applicables aux principes décrits aux points 2, 3, 4 et 5 ainsi qu'aux droits des personnes concernées (point 6) dans le cas d'objectifs spécifiques tels qu'indiqué ci-dessus.

Exemple : Si 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.

Si une exception telle qu'elle est définie par le droit national qui prévoit des garanties spécifiques est utilisée par la police, elle doit l'être pour des finalités légitimes et seulement dans la mesure où elle est nécessaire et proportionnée pour atteindre la finalité pour laquelle elle a été utilisée. Le but dans lesquels la police utilise ces exceptions devrait être limité aux cas où ces règles et principes

risqueraient de mettre en danger les tâches de police décrites au Point 1 ou mettrait en danger les actions menées aux fins figurant dans la liste des exceptions décrites ci-dessus.

Exemple : Si des renseignements particuliers prouvent que des opérations de blanchiment d'argent ont été menées pour financer des activités terroristes, les données collectées sur des individus peuvent être conservés pendant une période plus longue que celle qui serait autrement strictement nécessaire à la police pour une enquête, si cela est approuvé par l'organisme assurant le contrôle externe.

8. Utilisation de techniques d'enquête spéciales

En ce qui concerne l'utilisation de techniques spéciales d'enquête, la police est invitée à se référer à la Recommandation (2017)6 du Comité des Ministres aux Etats membres sur les "techniques spéciales d'enquête" en ce qui concerne les crimes graves, y compris les actes de terrorisme. En particulier, les paragraphes 7 à 10 de la recommandation peuvent donner des indications utiles sur l'application légale de ces techniques d'enquête.

Ce domaine est généralement régi en détail dans le droit procédural pénal national, mais au moment de décider de leur utilisation, certaines considérations relatives à la protection des données pourraient être évaluées afin de permettre à la police d'appliquer les moyens les moins intrusifs de traitement de données durant ses opérations. Si des mesures moins intrusives pour aboutir au but recherché existent, elles doivent être privilégiées. L'emploi de techniques spéciales d'enquête ne peut être considéré comme proportionné que si le même résultat ne peut être obtenu par des méthodes moins intrusives. Quelles que soient les méthodes d'enquête ou d'autres opérations menées par la police, celle-ci a l'obligation de se conformer aux principes généraux relatifs à la protection des données à caractère personnel décrits dans les Considérations générales, sauf dans les cas où la législation l'en dispense explicitement.

Les progrès techniques ont rendu la surveillance électronique plus facile, mais il ne faut pas oublier que leur utilisation peut constituer une ingérence dans les droits et libertés fondamentales, en particulier dans le droit au respect de la vie privée. Le choix de la méthode d'enquête doit donc s'accompagner d'une mise en balance du potentiel de risque élevé d'ingérence grave dans le droit à la protection de la vie privé avec la gravité de l'infraction à prévenir ou sur laquelle enquêter, la rentabilité, l'utilisation des ressources et l'efficacité de l'enquête.

Exemple : Dans une enquête, les preuves de la communication entre deux suspects peuvent être recueillies de diverses façons. Si des interrogatoires, des témoignages, l'obtention des données d'appels téléphoniques ou une surveillance discrète permettent d'obtenir le même résultat sans nuire à l'efficacité de l'enquête, ils doivent être préférés à l'utilisation de mesures de surveillances plus intrusives telles que les écoutes.

9. Introduction de nouvelles technologies de traitement des données

Si le traitement des données est susceptible d'affecter fortement les 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 au regard des actions envisagées. Considérant que l'introduction de nouvelles technologies de traitement des données présente en soi un tel risque potentiel, il est probable que l'introduction d'une telle technologie impliquera un EIPD. Il est recommandé que l'évaluation des risques ne soit pas statique mais qu'elle prenne en compte le cas spécifique, qu'elle soit répétée à intervalles raisonnables, qu'elle concerne les étapes pertinentes de l'activité de traitement des données et qu'elle prenne en compte les considérations de responsabilité. La pertinence de l'EIPD devrait être contrôlée à intervalles raisonnables.

En termes de sécurité des données et des communications, il est aussi très important que les normes les plus élevées soient prises en compte au moment d'introduire les nouvelles technologies.

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, ainsi que les risques qu'elles peuvent représenter pour les droits des personnes y compris en ce qui concerne la sécurité des données.

L'autorité de protection des données a un rôle important à jouer ; elle conseille sur les risques pour la protection des données et sur 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 et persistant d'atteinte aux droits de l'intéressé, en dépit de l'adoption de mesures de sauvegarde spécifiques.

Les consultations entre le responsable du traitement des données et l'autorité de contrôle devraient permettre à cette dernière d'avoir suffisamment d'opportunités de donner des avis motivé et faire une évaluation des activités du responsable du traitement des données sans compromettre ses fonctions essentielles.

Des renseignements appropriés devraient être fournis à l'autorité de protection des données, 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 traitées et qui y a accès. Il faut également fournir des informations sur la conservation des données et la politique applicable en matière d'enregistrement et d'accès ainsi que sur tous les aspects techniques de mise en œuvre.

Exemple : Des informations détaillées sur les fichiers nationaux de référence qui contiennent des données sur les empreintes digitales telles que la finalité ou le responsable du traitement des données, etc. devraient être indiquées ou mise à disposition de l'autorité de protection des données pour consultation.

À l'issue des consultations, le responsable du traitement doit soigneusement envisager de mettre en œuvre toute mesure et garantie nécessaire recommandée par l'autorité de protection des données.

Exemple : La mise en place d'un système de reconnaissance faciale automatique ou de tout autre système basé sur le traitement automatisé de données biométriques devrait très probablement nécessiter une consultation pour que les risques encourus par les droits de l'intéressé soient clairement définis. S'il le faut et si cela est recommandé par l'autorité de protection des données consultée sur la question, 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, les problèmes d'accès aux données, etc.) pour se conformer aux principes et dispositions de la protection des données.

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 par internet dans le cadre de leurs activités opérationnelles montrent que la technologie de l'internet des objets est déjà opérationnelle. En raison des vulnérabilités qu'elle peut présenter en matière de sécurité, cette technologie exige 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 connectées à une base de données nationale des casiers judiciaires. Il convient de garantir aux données collectées le plus haut niveau de sécurité.

Analyse des big data 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 pour les services de police qui décident d'utiliser des sources d'information numériques et des techniques de profilage pour accomplir leurs tâches.

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. Cela pourrait interférer avec le droit au respect de la vie privée et à la protection des données.

La Recommandation CM/Rec(2010)13 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage[3] et 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 des mégadonnées[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 toutefois important de tenir compte des risques considérables que présente cette forme de traitement de données :

- l'interprétation d'informations provenant de bases de données utilisées dans des domaines et contextes différents peut aboutir à des conclusions erronées et à des manques de base légales valides et de ce fait conduire à des traitements de données illégales 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 grave 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 porter une attention particulière aux exigences suivantes :

- la vérification de l'exactitude, du contexte et de la pertinence des données ;
- leur utilisation exige une forte obligation de rendre des comptes ;
- leur utilisation doit être combinée avec des méthodes d'enquête qui complètent des conclusions tirées de l'analyse des mégadonnées. Une décision qui affecte une personne ne doit pas être prise sur la seule base d'un traitement automatisé de données personnelles ;
- leur utilisation doit être nécessaire et proportionnée à l'accomplissement des tâches policières décrites au Point 1, avec une attention particulière à ce que les données ainsi traitées soient correctes, pertinentes et ne soient pas excessives par rapport au but poursuivi ;
- toute analyse prédictive nécessite une intervention humaine pour évaluer sa pertinence et les conclusions tirées ;
- des lignes directrices en matière d'éthique élaborées au niveau national ou international devraient être prises en considération ;
- comme principe et sous réserve des restrictions et dérogations mentionnées au Point 7, le responsable du traitement doit assurer la transparence en expliquant 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, il devrait normalement en informer les personnes concernées ;
- même dans le cas d'une utilisation de méthodes complexes, la légalité du traitement des données – y compris une utilisation secondaire – et sa conformité avec les conditions fixées par l'article 8 de la Convention européenne des droits de l'homme devraient être démontrées ;
- une politique de sécurité des informations doit être mise en place et appliquée tout au long du traitement ;
- les responsables du traitement devraient veiller à la loyauté du traitement des données à caractère personnel lorsque des big data servent de base à la prise de décisions qui ont des conséquences pour des individus et s'assurer que les voies administratives et judiciaires permettant de contester ces décisions existent. Cela implique que les personnes intéressées soient informées du mode opératoire des algorithmes utilisés ainsi que du but de leur utilisation.

Respecter les exigences mentionnées ci-dessus est particulièrement recommandé quand des

[3] Recommandation CM/Rec(2010)13 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

[4] Document T-PD(2017)1 – Lignes directrices

données sensibles sont traitées dans le cadre d'analyses de mégadonnées, en particulier celles portant sur l'intervention humaine et la combinaison de méthodes d'analyses nouvelles et traditionnelles.

10. Conservation des données

Comme énoncé au point 2, les données sont traitées tant qu'elles servent les fins pour lesquelles elles ont été collectées. Les données conservées devraient être correctes, actualisées, nécessaires, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées.

Des règles claires doivent être mises en place en ce qui concerne le traitement des différentes bases de données, avec une attention particulière portée à l'analyse des résultats des recherches donnants de résultats multiples.

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 nécessaires pour des finalités policières décrites au Point 1.

Les motifs de conservation et de traitement des données devraient être réexaminés périodiquement. Il est à noter que le traitement des données à caractère personnel en dehors du cadre légal prévu pour la conservation constitue une violation grave du droit à la protection de ces données. Si la loi relative à un crime spécifique prévoit une période de 4 ans de rétention des données, et si des données personnelles sont traitées par la police seulement en relation avec ce crime au-delà de 4 ans après leur collecte, qu'il n'existe aucune raison pour cela, la conservation des données en question serait considérée comme illégale.

Les périodes de conservation générales des données sont 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 qui fixent la durée de conservation des données à caractère personnel ou le réexamen régulier de la nécessité de leur conservation.

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 charges, ses données devront être 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 et si tous les délais de recours sont épuisés), pourvu aussi que tous les délais de révision de l'affaire aient également expiré. De même, si l'enquête est toujours en cours après 4 ans et que les données concernant cette personne restent pertinentes, la police devrait être en mesure de les conserver.

Dans ce dernier cas, il est 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 la fin de la procédure judiciaire (c'est-à-dire que 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.

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

Les données devraient dans la mesure du possible être classées 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 facilite 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 (autant que possible logiquement et physiquement) des données collectées à des fins policières. La police peut y accéder lorsque c'est nécessaire et autorisé par la loi.

Exemple : Parmi les données administratives figurent, par exemple, les listes de données relatives aux titulaires de licences ou les données relatives aux ressources humaines et aux permis de port d'arme.

11. Communication de données au sein de la police

Il convient de faire la distinction entre la communication de données sur le plan national au sein de la police (point 11) avec d'autres organismes publics (point 12) et le transfert international de données (point 14). Dans le cadre de ces opérations distinctes des obligations différentes s'appliquent en fonction du destinataire des données : la police, un autre organe public ou un tiers privé.

La communication de données entre services de police ne peut être permise que si elle est justifiée par un intérêt légitime dans le cadre des attributions légales de ces services (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 l'autorisant). Lors du partage de données au sein du secteur de la police, les droits des personnes concernées, tels que décrits au point 6, doivent bénéficier du même niveau de protection.

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

La police peut communiquer des données à d'autres services de police si ces données à caractère personnel sont nécessaires aux fins de prévention, d'enquête et de répression des infractions pénales et d'exécution des sanctions pénales [et lorsque les données à caractère personnel sont traitées dans le but du maintien de l'ordre public].

La communication de données à caractère personnel d'un service de police à l'autre doit être conforme aux considérations générales décrites ci-dessus, même si elle ne quittent pas la police.

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 ces crimes pourrait être la même personne ou si cette communication pourrait matériellement aider l'enquête.

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

La communication de données en dehors de la police est 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 accords d'entraide mutuelle prévus par la loi entre services chargés de l'application de la loi et organes publics permettent 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).

Des règles spécifiques devraient être respectées lorsque des données doivent être transmises à d'autres organismes nationaux que des services de police, car il y a un risque que le traitement de données personnel considérées comme données sensibles puisse avoir des conséquences dommageables à la personne concernée.

La communication de données à une autre autorité publique peut également être autorisée si elle est prévue par la loi, dans l'intérêt incontestable de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent pour d'autres personnes, 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 n'a jamais 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.

13. Communication de données par la police à des organismes privés

Il peut arriver dans des cas particuliers que, la police puisse communiquer des données à des organismes privés. Cette communication doit être prévue par la loi et être effectuée uniquement par l'autorité qui traite les données. Cela ne devrait être effectuée qu'aux fins d'une enquête ou d'autres missions importantes de la police telles que décrites au point 1, dans l'intérêt de la personne concernée, pour des raisons humanitaires ou si cela est nécessaire pour éviter un risque grave et imminent, pour l'ordre ou la sécurité publics et si un niveau approprié de protection tenant compte de la nature sensible des données de police est garanti. Par exemple il pourrait aussi y avoir des cas dans lesquels la police serait autorisée à communiquer des données à des organisations humanitaires sur le fondement du droit international, dans l'intérêt de la personne concernée ou pour des raisons humanitaires.

Lorsque la police communique des données aux médias afin de rendre publique des informations liées à une enquête, il importerait d'évaluer si cela est nécessaire et qu'une telle publicité soit permise dans l'intérêt public. Des garanties appropriées doivent être mises en place pour garantir le respect des droits des individus impliqués dans l'affaire.

Une telle communication ne devrait avoir lieu qu'au cas par cas et être chaque fois clairement prévue par la loi stipulant la procédure nécessaire à suivre pour cela (notamment la nécessité d'une autorisation spécifique).

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.

14. Transfert international

En règle générale tout transfert international de données de police devrait être limité à d'autres services de police, être adapté au but poursuivi et prévu par la loi. Cela implique également de suivre les procédures internes établies par le droit procédural pénal national qui peuvent inclure la participation active d'organismes et de services de l'ordre public plus larges, tels que Ministère de l'Intérieur, Ministère de la Justice, procureurs, juges d'instruction, etc. A cet effet, des 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 (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 effective.

Lorsqu'il est envisagé de partager des données, il conviendrait de vérifier si l'autorité destinataire a légalement une fonction qui vise des missions policières décrites au Point 1 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 à caractère personnel. Elle doit notamment prévoir des garanties appropriées 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 prises en compte [5] pour veiller à ce que tout transfert de données soit légalement justifié et soit encadré par des garanties suffisantes. Le demandeur doit clairement préciser tous les éléments nécessaires pour que la partie destinataire puisse prendre une décision fondée concernant la demande, notamment son motif ainsi que la finalité du transfert de données.

Il est nécessaire de s'assurer que des mesures appropriées sont en place pour protéger la sécurité de l'information et obtenir des assurances quant à l'utilisation qui en sera faite.

Un niveau de protection approprié des données devrait être garanti lorsque des données doivent être transférées vers des pays qui ne sont pas parties à la Convention 108 (par exemple, par des moyens de sauvegarde standardisés ad hoc ou approuvés prévus par des instruments juridiquement contraignants et applicables par des accords, MoU, contrat, etc.).

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 policières décrites au Point 1 et si ce deuxième destinataire est également un service de police garantissant un niveau approprié de protection des données. Le service de police y compris les services du ministère public et / ou les juges d'instruction 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 l'accepte. Si les données sont communiquées à un pays Z qui n'est pas partie à la Convention 108, le pays Y doit veiller à ce que ce pays offre un niveau de protection appropriée des données à caractère personnel y compris l'existence des moyens effectifs pour l'exercice des droits correspondants des personnes concernées.

Le transfert international de données à caractère personnel à un service public 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 émettrice et s'il n'existe aucun autre moyen efficace de transférer les données à un service de police compétent. Les principes de protection des données énoncés dans la Convention 108 doivent être respectés pour tous les types de transferts, en particulier ceux liés à l'exigence d'un niveau de protection approprié qui prenne en compte le caractère sensible des données de police.

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 cette personne participe à des affaires criminelles dans le pays X, si la législation nationale le permet (par exemple sur la base d'un accord bilatéral sur l'évasion fiscale entre les deux pays) la police peut transférer les données à caractère personnel de la personne concernée.

En règle générale, le transfert international de données à caractère personnel entre la police et des organismes privés résidant dans une juridiction différente devrait être évité. Cela ne peut avoir lieu que dans des cas très exceptionnels dans lesquels cela est absolument nécessaire pour l'accomplissement des fonctions de police telles que décrites au point 1, si cela est prévu par des voies légales, et si un niveau approprié de protection tenant compte de la nature sensible des données de police est garanti. Les facteurs supplémentaires à prendre en compte pour un tel transfert sont l'urgence de la situation, la nature du crime, son caractère transfrontalier et quand l'implication éventuelle de la police locale pourraient nuire à l'objet de l'enquête pour des raisons objectives.

[5] Cela est sans préjudice du droit du Comité de la Convention 108, et d'autres instances disposant de ce pouvoir, d'évaluer et de réexaminer si nécessaire le niveau de protection des données garanti par ces accords multilatéraux.

D'autres faits tels que la sécurité des données, l'assurance reçue relative à l'utilisation des données et la licéité du transfert des données dans le pays destinataire doivent être pris en compte. Dans ce contexte, il convient de noter que, dans un tel cas, le responsable du traitement des données a une double obligation en ce qui concerne la protection des données à caractère personnel : celle imposée par le cadre juridique de son pays de résidence et celle liée au transfert de données. La police locale devrait 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. Des transferts internationaux sont aussi exceptionnellement possibles quand la police communique des données à caractère personnel à des fins humanitaires.

Exemple : Dans une enquête menée dans le cadre d'un accord international multilatéral sur du matériel pédopornographique diffusé sur internet, la victime est dans le pays Y et la police y compris les services de procureur général y a commencé une enquête mais le suspect ayant mis en ligne ce matériel réside dans un autre pays (pays X), le risque est élevé que la personne cherche à fuir le pays X. Dès lors, la police du pays Y peut demander à un fournisseur de services internet 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.

15. Conditions de la communication

Dans la mesure où le responsable du traitement a l'obligation générale de veiller à une haute qualité des données, il est souhaitable de procéder à une vérification supplémentaire avant de communiquer des données à d'autres organismes. Tout partage ou transfert de données doit s'accompagner d'un contrôle rigoureux de leur qualité : leur exactitude, leur actualité, leur pertinence et leur exhaustivité. Autant que possible, les décisions judicaires ainsi que les décisions de ne pas poursuivre devraient être indiquées lors de toute communication de données. Des canaux de communication sûrs doivent être mis en place afin d'assurer une sécurité des données au plus haut niveau possible. La qualité des données peut être évaluée jusqu'au moment de la communication.

Exemple : Si des données à caractère personnel qui contiennent des données erronées (personnelles ou autres) sont envoyées, elles peuvent négativement affecter l'enquête, causer préjudice à la personne concernée ou à d'autres personnes impliquées ou qui pourraient l'être du fait d'un transfert de données incorrectes. Cela peut entraîner la responsabilité de l'État expéditeur comme celle de l'État receveur. L'arrestation d'une personne du fait de la mauvaise communication du nom d'un suspect porte gravement atteinte à plusieurs droits de l'homme de la personne concernée et peut affecter l'enquête pénale.

16. Garanties concernant la communication

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

Aucune donnée partagée ne devrait être utilisée à d'autres fins que celles pour lesquelles elle a été communiquée ou reçue. Les seules exceptions à cela sont lorsque l'autorité expéditrice donne, sur une base légale, son accord pour une autre utilisation et si cela est nécessaire et indispensable pour que le destinataire accomplisse sa tâche. Les données peuvent également être communiquées si cela est dans l'intérêt de la personne concernée, pour des raisons humanitaires, ou encore si cela est nécessaire pour prévenir un risque grave et imminent à l'ordre public ou à la sécurité publique et qu'un niveau approprié de protection des données est garanti par le destinataire au moyen d'un instrument juridique international ou national, ou par des moyens de sauvegarde standardisés ad hoc ou approuvés prévus par des instruments juridiquement contraignants et applicables, tels que des accords, des MoU, des contrats, etc., comme le prévoit la Convention 108.

Exemple : Des données à caractère personnel envoyées par la police d'un pays X à la police d'un pays Y dans un cas de blanchiment d'argent ne peuvent pas être utilisées par des policiers pour 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).

17. 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 conservées dans différents fichiers ou bases de données détenus à des fins variées, par exemple des fichiers conservés par d'autres organismes publics ou privés. Ces recoupements peuvent être en relation avec une enquête pénale 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 si la législation nationale, qui doit prendre en compte les principes fondamentaux de la protection des données, le permet.

Une législation et des indications claires, conformes aux principes de protection des données, doivent être en place pour encadrer ces croisements de bases de données. De tels croisements devraient être nécessaires, servir une finalité précise et être proportionnés.

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

18. Sécurité des données

La police doit prendre des mesures adéquates de sécurité 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. Lors de l'examen de la sécurité des données, la police devrait également prendre en compte des facteurs tels que la localisation des données, la certification adéquate des fournisseurs de services et l'assurance de la disponibilité des données. Il est également conseillé de faire attention à la sécurité des données lors de la distribution des droits d'accès. Le responsable du traitement doit, au minimum, informer sans délai l'autorité de contrôle compétente des violations de données qui, selon son jugement, peuvent gravement porter atteinte aux droits et libertés fondamentales des personnes concernées. Les personnes concernées par des violations de leurs données qui peuvent gravement porter atteinte à leurs droits doivent être informées sans délais superflu, sauf si cela présente un risque pour les activités de la police.

La sécurité des informations est essentielle à la protection des données. Il s'agit d'un ensemble de procédures destinées à garantir l'intégrité, la disponibilité et la confidentialité 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'impact des incidents de sécurité et violations des données 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 les informations sensibles devraient systématiquement être cryptées. 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 le cas échéant à une évaluation de l'impact sur la protection des données personnelles (EIPD) (voir point 4) afin d'évaluer les risques pour les droits de la personne concernée découlant 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. Une telle évaluation doit porter sur les systèmes et procédures pertinents des opérations de traitements et non sur des cas individuels.

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

Il peut être recommandé d'utiliser un système de gestion de l'identité et des accès (IAM) 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 peut être considéré comme une condition utile pour garantir un accès sécurisé et correct aux données.

Après une évaluation des risques, le responsable du traitement des données devrait mettre en œuvre les mesures appropriées destinées entre autre 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 (« privacy by design »)

Le concept du respect de la vie privée dès la conception fait partie intégrante de la sécurité des données. La protection et la sécurité des données peuvent être directement intégrées dans les systèmes et processus d'information, au moyen de mesures techniques et organisationnelles, afin d'assurer un niveau élevé de protection et de sécurité des données et, en particulier, de réduire au minimum le risque de violation. Cette approche, appelée « respect de la vie privée dès la conception », favorise dès le début la prise en compte de 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 finalités.

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 (PETs) afin de permettre une meilleure protection des données à caractère personnel. Ces technologies empêchent le traitement excessif des données à caractère personnel sans réduire les capacités fonctionnelles du système informatique.

Exemple : Les scanners corporels utilisés à des fins policières doivent être conçus pour respecter la vie privée des individus inspectés 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 d'assurer et de veiller à la conformité du traitement des données avec la législation nationale et internationale dans le secteur de la police.

Certains États 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 ni être dirigé par un autre organe dépendant de la partie exécutive d'une administration nationale. Il devrait disposer des ressources suffisantes pour exécuter ses tâches et fonctions et ne devrait recevoir aucune instruction d'où qu'elle vienne. L'indépendance personnelle de son président, politique aussi bien que financière, fonctionnelle et opérationnelle, est un critère essentiel lorsqu'il s'agira d'en évaluer l'indépendance.

La législation nationale devrait conférer à cet organe des pouvoirs de conseils, d'enquête et des pouvoirs répressifs lui permettant d'enquêter à la suite de plaintes, d'appliquer des mesures réglementaires ou d'infliger des sanctions le cas échéant. Les outils juridiques et administratifs à sa disposition doivent être efficaces et il devrait pouvoir faire appliquer ses décisions.

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 indépendante et doit 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 unique ou son authentification ;

d) « donnés subjectives » (preuves fondées sur un témoignage ou une déclaration personnelle) : données acquises par le biais de témoignages de personnes impliquées dans l'enquête ;

e) « données objectives » (preuves fondées sur des documents ou des faits avérés) : données acquises provenant de documents officiels ou d'autres sources certifiées ;

f) « traitement de données » : toute opération ou ensemble d'opérations effectuée 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 effectuée sur des données à caractère personnel présentes dans un ensemble structuré de ces données qui sont accessibles ou récupérables selon des critères spécifiques ;

g) «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 ;

h) « 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 ;

i) «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 ;

j) « internet des objets » (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 ;

k) « surveillance secrète » : 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 ;

l) « 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 ;

m) « technologies de renforcement de la protection de la vie privée » (PETs) : diverses technologies utilisées pour protéger les données personnelles au sein de systèmes d'information. L'aspect le

plus important dans l'utilisation des PETs est de déterminer au moment du développement ou de la conception d'un nouveau système d'information ou de la mise à jour d'un système existant si une information identifiable est nécessaire.