COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 17 mai 2016 T-PD(2016)02rev

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL

(T-PD)

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

Direction générale Droits de l'homme et Etat de droit

Introduction

La Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police précise clairement que l'organe responsable des données au sein de la police peut uniquement procéder à leur traitement dans un but légitime, expressément précisé au moment de leur collecte, et peut uniquement utiliser ces données à des fins compatibles avec le but initialement poursuivi par leur collecte.

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 des données à caractère personnel par la police dans l'ensemble de l'Europe. Cette dernière évaluation a souligné que les principes énoncés par la Recommandation (87)15 étaient toujours pertinents et continuaient à offrir un fondement solide et actualisé pour l'élaboration d'une réglementation nationale en la matière.

Lors de sa 31e réunion plénière en 2014, le Comité consultatif a réaffirmé que la Recommandation (87)5 ne serait pas révisée et a chargé son Bureau d'analyser les besoins dans ce domaine et les solutions normatives envisageables, en tenant compte des travaux en cours du Comité de la Convention sur la cybercriminalité (T-CY) et du Comité d'experts sur le terrorisme (CODEXTER).

À la suite du mandat donné par le Comité consultatif, le Bureau a examiné les besoins et les options possibles des travaux consacrés à l'utilisation des données à caractère personnel par la police et a décidé de proposer élaboration d'un guide pratique de l'utilisation des données à caractère personnel par la police, sur la base des principes énoncés par la Recommandation (87)15 et en fournissant des éléments d'orientation clairs et concrets sur ce que ces principes impliquent au niveau opérationnel.

Un groupe d'experts[2] a été chargé d'élaborer le projet de guide pratique. Celui-ci a été présenté lors de la 38e réunion du Bureau (22-24 mars 2016) et révisé par la suite. Il est soumis aux délégations et aux observateurs du Comité consultatif, ainsi qu'aux autres parties prenantes concernées, pour adoption lors de la 33e réunion plénière du Comité consultatif (du 29 juin au 1er juillet 2016).

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

[2] Mme Evelien van Beek (conseillère principale, Autorité de protection des données, Pays-Bas) et M. David Allen (chef du Bureau de la criminalité internationale, Direction du renseignement et des opérations, Agence de lutte contre la criminalité (National Crime Agency), Royaume-Uni). M. John Borking (consultant indépendant, Pays-Bas) a contribué à la rédaction de la partie consacrée à la sécurité des données.

Principe 1 – Contrôle et notification

1.1. Chaque Etat membre devrait disposer d'une autorité de contrôle indépendante et extérieure à la police, chargée de veiller au respect des principes applicables en matière de protection des données.

Il importe de noter que le traitement des données à caractère personnel devrait uniquement intervenir lorsqu'il fait l'objet d'une loi qui en établit la procédure et l'obligation.

Chaque État membre doit disposer d'une autorité de contrôle indépendante chargée de contrôler le traitement des données à caractère personnel par la police. Certains États membres peuvent exiger la présence de plusieurs autorités de contrôle, par exemple une autorité nationale ou fédérale et un certain nombre d'autorités décentralisées ou régionales.

L'autorité de contrôle ou l'Autorité de protection des données (APD) doit être totalement indépendante de tout autre autorité publique ou privée. Pour être efficace, il importe que l'ADP dispose de ressources suffisantes – budgétaires et en personnel – pour mener à bien sa mission en toute indépendance. La jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne démontre l'importance de cette question.

L'APD doit disposer de pouvoirs suffisants pour lui permettre de procéder à ses contrôles de manière efficace et indépendante. Il importe que la législation nationale lui confère des pouvoirs d'enquête et des pouvoirs répressifs, afin qu'elle puisse mener une enquête à la suite d'une plainte et mettre un terme au traitement illégal de données à caractère personnel ou infliger des sanctions si besoin est. Il est recommandé de conférer à l'APD des pouvoirs de sanction du traitement illégal des données.

1.2. L'introduction de nouveaux moyens techniques pour le traitement de données ne devrait être admise que si toutes les mesures raisonnables ont été prises pour s'assurer que leur utilisation est conforme à l'esprit de la législation existante sur la protection des données.

Lorsque la police dispose de nouveaux moyens techniques – informatisés ou autres – qu'elle peut utiliser pour le traitement des données à caractère personnel, l'organe responsable des données devrait en apprécier la conformité avec la législation relative à la protection des données. Si le traitement risque très probablement de porter atteinte aux droits de l'intéressé, il importe que l'organe responsable des données procède à une Évaluation de l'impact de la protection des données (EIPD), afin d'apprécier l'ensemble des risques que ce traitement présente pour la protection des données à caractère personnel.

Exemple :
les nouvelles techniques d'exploration des données peuvent offrir des possibilités étendues de sélection des suspects éventuels et il convient d'évaluer soigneusement leur conformité avec la législation en vigueur en matière de protection des données.

1.3. L'organe responsable devrait consulter à l'avance l'autorité de contrôle chaque fois que l'introduction de procédés de traitement automatisé soulève des questions en matière de protection des données.

L'APD a un rôle important à jouer : elle doit indiquer les risques que ce traitement automatisé présente pour la protection des données et les garanties qu'il convient de mettre en place pour veiller à ce que tous les moyens techniques soient conformes avec la législation relative à la protection des données. Avant de procéder au traitement des données dans un nouveau système, notamment lorsqu'on fait appel aux nouvelles technologies, l'organe responsable

des données devrait consulter l'APD chaque fois que l'évaluation des risques ou l'EIPD démontre l'existence d'un risque élevé d'atteinte aux droits de l'intéressé.

La méthodologie de la consultation de l'APD par l'organe responsable des données doit être définie de manière à permettre suffisamment à l'APD de donner son avis motivé et une évaluation du traitement des données par l'organe responsable des données, sans compromettre ses fonctions essentielles. À l'issue de cette consultation, l'organe responsable des données met en œuvre les mesures et les garanties nécessaires avant de procéder au traitement des données.

Exemple :
la mise en place d'un système de reconnaissance faciale automatique doit faire l'objet d'une consultation pour que les risques imminents encourus par les droits de l'intéressé soient clairement indiqués. Si besoin est, il convient d'ajouter des garanties particulières qui permettront d'assurer la conformité, le traitement équitable et la sécurité des informations.

1.4. Les fichiers permanents automatisés devraient être déclarés à l'autorité de contrôle. Cette déclaration devrait spécifier la nature de chaque fichier déclaré, l'organe responsable de ce traitement, ses finalités, les types de données qu'il contient et les destinataires auxquels les données sont communiquées.

Les fichiers ad hoc, constitués à l'occasion d'affaires particulières, devraient également être déclarés à l'autorité de contrôle soit dans des conditions arrêtées avec celle-ci eu égard à leur spécificité, soit conformément à la législation nationale.

Les fichiers permanents peuvent être créés pour différentes catégories de traitement des données, en fonction des besoins et des exigences de la police. Il convient de déclarer ces fichiers à l'APD lorsque ce type de fichier n'est pas encore pris en compte par une législation particulière en vigueur. Chaque déclaration doit préciser le type de fichier, l'organe responsable des données, la finalité de ces données, le type de données qui figurent dans le fichier et les destinataires des données, ainsi que 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, par exemple leur finalité ou l'organe responsable des données, doit être indiquée à l'APD.

Les fichiers ad hoc ou temporaires créés pour une occasion particulière ou pour une enquête précise doivent être établis dans le respect de la législation applicable en matière de protection des données. Il importe de déclarer l'existence de ces fichiers conformément à ce que prévoit la législation nationale ou de les déclarer, soit à l'APD, soit à l'agent interne chargé de la protection des données si celui-ci a pour mission de contrôler le respect de la législation nationale. Lorsqu'il s'agit d'un fichier ad hoc, la déclaration doit mentionner l'organe chargé du traitement des données, la finalité du fichier, les catégories de données qui peuvent être traitées, et notamment le caractère sensible des données et/ou le délai de conservation des données ou les conditions auxquelles les données peuvent être transmises à leurs destinataires.

La législation nationale peut prévoir qu'aucune déclaration n'est nécessaire ou que seuls certains types de fichiers doivent être déclarés, sans qu'il soit besoin de déclarer chaque enquête ou opération menée dès son ouverture.

Exemple :

lorsqu'une enquête est menée sur une infraction ou un groupe de malfaiteurs, des précisions peuvent être données, par exemple, sur la finalité des données, l'organe responsable des données ou les catégories de données traitées, à l'agent chargé de la protection des données au sein du service répressif, afin que les données pertinentes soient constamment accompagnées de ces renseignements.

Principe 2 - Collecte des données

2.1. La collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique.

Le traitement des données à caractère personnel à des fins de police constitue une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. Cette ingérence doit par conséquent se fonder sur des dispositions claires et publiquement disponibles et se limiter à ce qui est nécessaire dans une société démocratique.

L'obtention de données à caractère personnel doit être clairement utile à une enquête. Il convient de collecter uniquement le minimum de données nécessaires au but poursuivi.

Exemple :
en cas d'écoutes téléphoniques, les forces de l'ordre devraient uniquement demander la quantité d'écoutes téléphoniques nécessaire à la période qui fait l'objet de l'enquête.

Il importe que les données soient uniquement collectées pour prévenir, déceler ou enquêter sur une infraction pénale. La définition d'un danger concret ou d'une infraction pénale déterminée a été étendue : elle englobe le soupçon d'activités criminelles qui ont déjà eu lieu ou qui devraient avoir lieu à l'avenir.

Exemple :
lorsque des renseignements permettent de savoir qu'un service précis de transfert de capitaux a servi au blanchiment de capitaux, la collecte de données relatives aux propriétaires et aux clients de cette activité précise peut se justifier. Mais ces éléments ne sauraient justifier la collecte de données portant sur les propriétaires et clients de tous les services de transfert de capitaux de la ville.

Toute exception à cette règle doit être prévue par la législation nationale.

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

2.2. Lorsque des données concernant une personne ont été collectées et enregistrées à son insu, elle devrait, si les données ne sont pas détruites, être informée, si cela est possible, que des informations sont détenues sur son compte, et ce, dès que l'objet des activités de police ne risque plus de subir un préjudice.

Cette situation concerne les personnes qui font l'objet d'une surveillance ciblée discrète et/ou d'une enquête, et non les personnes filmées au moyen de techniques de surveillance à grande échelle, comme la vidéosurveillance.

Lorsque des données relatives à une personne ont été collectées au cours d'une enquête dont elle est le suspect, il importe que la police informe l'intéressé du traitement des données dès que la situation le permet.

La police n'a pas à faire cette démarche si elle estime que le fait de communiquer cette information à l'intéressé peut être préjudiciable à l'enquête, parce qu'il lui permettra de prendre la fuite ou de détruire des éléments de preuve.

Il convient de détruire immédiatement les données qui ne sont pas utilisées.

Il peut arriver que la conservation des données pendant une longue durée se justifie et que le fait d'en informer la personne qui en fait l'objet soit préjudiciable. La conservation prolongée de ces données doit se justifier par des raisons valables. Il convient de réexaminer périodiquement les motifs de conservation et de traitement des données.

Exemple :
le traitement prolongé des données et la conservation prolongée de celles-ci peuvent se justifier pour procéder à la surveillance discrète d'un délinquant sexuel à haut risque, sous réserve que ces données soient nécessaires à cette fin.

2.3. La collecte de données par le biais de moyens techniques de surveillance ou d'autres moyens automatisés devrait être prévue dans des dispositions spécifiques.

Il convient de procéder à la collecte de données par le biais de moyens techniques de surveillance ou d'autres moyens automatisés uniquement si la législation le permet. La police et les autres services répressifs doivent agir dans le cadre de la loi, qui doit au minimum être conforme aux dispositions de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

L'article 8 de la Convention consacre un droit général au respect de la vie privée et familiale et prévoit un cadre de réglementation de la surveillance de l'utilisation des données respectueux de la vie privée. L'ingérence dans ce droit est uniquement possible conformément au droit interne et si elle constitue une mesure nécessaire à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la morale ou à la protection des droits et libertés d'autrui.

Il convient de réexaminer régulièrement la jurisprudence de la Cour européenne des droits de l'homme applicable à la collecte des données par le biais de moyens techniques de surveillance. La jurisprudence antérieure a précisé que ces formes de surveillance technique devaient être autorisées et faire l'objet de garanties contre les abus. Il importe également de réexaminer la jurisprudence applicable à l'arrestation ou la détention à des fins d'interrogatoire, aux perquisitions et aux saisies, aux méthodes d'interrogatoire, au prélèvement d'échantillons corporels ou à la prise d'éléments biométriques, car ces mesures doivent également être conformes à la législation nationale pertinente et aux dispositions de la convention, selon l'interprétation retenue par la Cour européenne des droits de l'homme.

Nul ne devrait faire l'objet de mesures ou de décisions ayant d'importantes conséquences judiciaires pour lui sur la base d'un traitement automatisé des données, sauf si la législation nationale le permet et que les garanties applicables sont suffisantes pour protéger les droits et les intérêts légitimes de l'intéressé. Celui-ci doit être dûment informé du type de traitement utilisé et cette information doit lui être donnée de manière claire et intelligible, afin de lui permettre de comprendre la logique du traitement appliqué.

L'internet des objets est constitué par la connexion en réseau des objets physiques, tels que les dispositifs, véhicules, bâtiments et autres objets qui intègrent de l'électronique et des

logiciels permettant de collecter et de mettre en commun des données. Les données transmises à la police et à ses agents ou par ceux-ci dans le cadre de leurs activités opérationnelles (par exemple GPS et caméras corporelles) au moyen d'internet peuvent être vulnérables. L'internet des objets exige la prise de mesures, comme l'authentification des données, leur intégrité ou le contrôle de l'accès aux données et la protection des données, de manière à pouvoir résister aux cyber-attaques.

Les mégadonnées et le profilage dans les services de police
L'augmentation constante de la place du numérique dans notre existence entraîne une augmentation des données à caractère personnel générées, collectées et partagées au moyen d'internet. Les avancées technologiques obtenues sur le plan du traitement et de l'analyse d'ensembles de données importants et complexes qui conduisent à la constitution de mégadonnées, ainsi que l'analyse de ces mégadonnées, offrent des possibilités aux services de police, mais engendrent également des difficultés auxquelles ils se heurtent, ce qui les amène à se tourner vers des sources d'information numériques et des techniques de profilage pour accomplir leur mission judiciaire.
Les technologies des mégadonnées permettent la collecte en vrac et l'analyse d'une immense quantité de données générées par les communications et les dispositifs électroniques associés à d'autres données en vrac. Ce mode de traitement des données risque d'entraîner une ingérence collatérale, qui peut avoir des répercussions sur les droits fondamentaux d'une personne, comme le droit au respect de la vie privée et à la protection des données.

Les technologies des mégadonnées et les techniques d'analyse peuvent aider à la découverte d'une infraction, mais il convient de tenir compte des risques considérables que présente cette forme de traitement des données.

- L'utilisation, dans un domaine, de bases de données provenant d'un autre domaine, dont le contexte est différent, peut conduire à l'établissement de conclusions erronées.
- Ces conclusions erronées peuvent avoir de graves conséquences pour les intéressés, surtout au sein des services de police, où l'organe responsable des données agit sans transparence et où les informations demeurent confidentielles.
- Le profilage peut entraîner l'établissement de conclusions discriminatoires ou injustes, susceptibles de renforcer les préjugés, la stigmatisation et la discrimination qui en découlent.
- La quantité croissante de données sensibles et confidentielles détenues par les services de police peut entraîner une vulnérabilité de leurs bases de données et, par voie de conséquence, une violation des données lorsque la sécurité de ces informations n'est pas garantie.

En cas d'utilisation de données à caractère personnel, l'organe responsable des données doit veiller à respecter les obligations nées des principes applicables en matière de protection des données et tenir dûment compte des exigences suivantes.

- La qualité des données utilisées dans le traitement des mégadonnées est une condition préalable essentielle ; la vérification de l'exactitude, du contexte et de la pertinence des données s'impose.
- L'organe responsable des données doit faire preuve de 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 compatible, il importe que l'organe responsable des données informe ses utilisateurs de cette utilisation secondaire.
- Il convient de démontrer 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.
- Il importe de mettre en place une politique de sécurité des informations.
- L'analyse des mégadonnées et le traitement des résultats de cette analyse doivent être effectués par des personnes expertes en la matière.

- L'organe responsable des données doit veiller à l'équité du traitement des données à caractère personnel lorsque la prise de décisions qui ont des conséquences pour les intéressés repose sur l'utilisation des mégadonnées.

2.4. La collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée. La collecte de données concernant ces facteurs ne peut être effectuée que si elle est absolument nécessaire pour les besoins d'une enquête déterminée.

La collecte de données à caractère personnel sur des individus au seul motif de :
- leurs origines raciales ou ethniques
- leurs croyances religieuses et convictions
- leur vie ou orientation sexuelle
- leurs opinions politiques ou de
- leur appartenance à une organisation ou à un mouvement particulier, comme l'adhésion à un syndicat,

devrait être interdite, sauf si cette collecte est strictement nécessaire aux besoins d'une enquête précise. Ce principe vaut également pour les données à caractère personnel qui concernent la santé et les données génétiques ou biométriques.

Cette collecte doit être conforme à la législation nationale et à l'article 8 de la Convention européenne des droits de l'homme. L'interdiction du motif de comportement sexuel n'est pas applicable lorsqu'une infraction a été commise.

Exemple :
le traitement des données au seul motif de la croyance religieuse d'un individu n'est pas autorisé. Mais dans le cadre d'une enquête portant sur un groupe de personnes susceptibles de mener des activités terroristes en raison de leurs convictions islamistes djihadistes, le traitement de ces données revêt une importance capitale.

Principe 3 - Enregistrement des données

3.1. Dans la mesure du possible, l'enregistrement de données à caractère personnel à des fins de police ne devrait concerner que des données exactes et se limiter aux données nécessaires pour permettre aux organes de police d'accomplir leurs tâches légales dans le cadre du droit interne et des obligations découlant du droit international.

Pour permettre à la police d'accomplir sa mission efficacement, les données à caractère personnel collectées à des fins de police doivent être enregistrées selon des critères précis, en fonction de leur nature (données subjectives ou objectives, par exemple) et de leur classification.

Toute donnée enregistrée devrait être adéquate, pertinente et ne pas être excessive par rapport à la finalité de sa collecte. L'exactitude et la fiabilité des données sont essentielles pour permettre à la police d'accomplir sa mission.

Il importe que la police prévoie des systèmes et des mécanismes pour que les données enregistrées soient aussi exactes que possible et que leur intégrité soit préservée. Le principe du respect de la vie privée dès l'élaboration de ces systèmes et mécanismes peut permettre d'y parvenir. Parallèlement, les droits et libertés des personnes doivent être pleinement pris en compte.

La structure des fichiers et la qualité des données enregistrées qui y figurent doivent être conformes à toutes les obligations légales, nationales et internationales. Les obligations internationales imposent la transmission de données à des organes internationaux comme Europol, Eurojust et INTERPOL, ainsi que l'existence d'accords bilatéraux et d'une entraide judiciaire entre États membres.

3.2. Les différentes catégories de données enregistrées devraient être différenciées, dans la mesure du possible, en fonction de leur degré d'exactitude ou de fiabilité et en particulier les données fondées sur des faits devraient être différenciées de celles fondées sur des opinions ou appréciations personnelles.

Il convient de classer les données par catégorie en fonction de leur degré d'exactitude et de fiabilité, afin d'aider la police à mener à bien 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.

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.

La classification des données est également importante lorsqu'elles doivent être communiquées à d'autres services de police ou à d'autres États.

Le classement des données à caractère personnel par la police doit établir une distinction claire entre les différentes catégories de personnes, comme les suspects, les personnes condamnées pour une infraction pénale, les victimes et les tiers, par exemple les témoins. Cette distinction doit 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'avoir commis une infraction pénale ou qui n'ont pas été condamnées pour la commission d'une infraction pénale.

3.3. Lorsque des données qui ont été collectées à des fins administratives sont destinées à un enregistrement permanent, elles devraient être enregistrées dans un fichier séparé. En tout cas, des mesures devraient être prises pour que les données administratives ne soient pas soumises aux règles applicables aux données de police.

Les données de police de nature administrative, c'est-à-dire les données qui ne sont pas utilisées pour prévenir, déceler ou enquêter sur des infractions pénales, doivent être enregistrées séparément, car elles ne peuvent être soumises aux mêmes dispositions que les données collectées à des fins de police.

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.

Principe 4 – Utilisation des données par la police

4. Sous réserve du principe 5, les données à caractère personnel collectées et enregistrées par la police à des fins de police devraient servir exclusivement à de telles fins.

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

Le traitement des données à caractère personnel d'une manière incompatible avec la finalité précisée au moment de leur collecte est illégal et n'est pas autorisé.

Principe 5 - Communication des données

5.1. Communication au sein de la police

La communication de données entre services de police en vue d'une utilisation à des fins de police ne devrait être permise que s'il existe un intérêt légitime à cette communication dans le cadre des attributions légales de ces services.

Il importe que les autorités policières communiquent uniquement leurs informations lorsque la demande qui leur en est faite est prévue par la loi, par exemple en cas d'enquête judiciaire en cours ou en cas de mission de police partagée.

5.2.i. Communication à d'autres organes publics

La communication de données à d'autres organes publics ne devrait être permise que, si dans un cas déterminé :
a. il y a obligation ou autorisation légale claire ou autorisation de l'autorité de contrôle, ou si
b. ces données sont indispensables au destinataire pour accomplir sa tâche légale propre et pour autant que le but de la collecte ou du traitement exécuté par ce destinataire n'est pas incompatible avec celui prévu à l'origine et que les obligations légales de l'organe communiquant ne s'y opposent pas.

5.2.ii. Une communication est, en outre, exceptionnellement permise si, dans un cas déterminé :
a. la communication est, sans aucun doute, dans l'intérêt de la personne concernée et si, soit celle-ci y a consenti, soit les circonstances permettent de présumer sans équivoque un tel consentement, ou si
b. la communication est nécessaire pour éviter un danger grave et imminent.

La communication de données hors des services de police est soumise à des principes plus stricts, car elle pourrait servir à d'autres fins qu'à des fins de police.

La communication des données à d'autres organes publics est uniquement autorisée si elle est prévue par la législation, par exemple si elle est autorisée par un juge, par des dispositions légales particulières ou par l'autorité de contrôle (voir le principe 1).

L'entraide entre la police et les organes publics permet à ces derniers d'avoir accès à des données de police essentielles à leur enquête ou à leurs autres attributions légales.

Exemple :
les autorités douanières lorsqu'elles enquêtent sur une fraude fiscale ou les autorités compétentes en matière d'immigration lorsqu'elles enquêtent sur une demande d'asile.

Les données communiquées peuvent uniquement être utilisées par l'organe destinataire aux fins pour lesquelles ces données ont été communiquées. La communication à une autre autorité publique est également autorisée si elle est indubitablement faite dans l'intérêt de la personne qui fait l'objet de ces données et si l'intéressé y a consenti.

Exemple :
lorsqu'un migrant fait une demande aux services de sécurité sociale, ces derniers peuvent avoir besoin des données détenues par la police pour vérifier le statut juridique de l'intéressé. La communication de ces données serait donc conforme à l'intérêt des services de sécurité sociale et de l'auteur de la demande.

La communication de données est également autorisée lorsqu'elle est conforme à l'intérêt général ou nécessaire à la prévention d'un grave danger.

5.3.i. Communication à des personnes privées

La communication de données à des personnes privées ne devrait être permise que si, dans un cas déterminé, il y a obligation ou autorisation légale claire ou autorisation de l'autorité de contrôle.

5.3.ii. Une communication à des personnes privées est exceptionnellement permise si, dans un cas déterminé :
a. la communication est, sans aucun doute, dans l'intérêt de la personne concernée et si, soit celle-ci y a consenti, soit les circonstances permettent de présumer sans équivoque un tel consentement, ou si
b. la communication est nécessaire pour éviter un danger grave et imminent.

Il peut arriver que la police ait besoin de communiquer des données à des organismes privés.

Exemple :
lorsque la police communique avec le secteur financier à propos de l'auteur d'une fraude ou d'un vol, ou avec une compagnie aérienne au sujet de documents de voyage volés ou perdus.

Cette communication de données doit être considérée comme exceptionnelle et doit être clairement prévue par la loi ou faire l'objet d'une autorisation.

Le principe 5.3 reprend les conditions fixées au principe 5.2.ii.

5.4. Communication internationale

La communication de données à des autorités étrangères devrait se limiter à des services de police. Elle ne devrait être permise que :
a. s'il existe une disposition légale claire découlant du droit interne ou international,
b. si, à défaut d'une telle disposition, la communication est nécessaire à la prévention d'un danger grave et imminent ou à la répression d'une infraction pénale grave de droit commun, et dans la mesure où il n'est pas porté atteinte aux réglementations internes relatives à la protection de la personne concernée.

Toute communication internationale de données à caractère personnel devrait uniquement intervenir si elle est clairement prévue par la loi. Le paragraphe 5.4b est uniquement applicable si l'État destinataire n'est pas membre d'Interpol ou s'il n'est pas partie à un traité qui autorise cette communication.

Toute communication internationale de données devrait être strictement limitée à d'autres services de police et conforme aux accords internationaux d'entraide, à la coopération prévue dans le cadre d'Interpol, d'Europol et d'Eurojust ou à tout autre accord bilatéral prévoyant une coopération et une communication efficaces.

Dans certains États membres, les activités de police sont en partie exercées par des autorités non policières. Le terme « services de police » doit s'entendre au sens large et peut englober d'autres pouvoirs publics chargés des enquêtes judiciaires.

Lorsqu'une communication de données est envisagée, il convient de vérifier systématiquement si l'autorité destinataire exerce une activité qui vise à prévenir, déceler ou enquêter sur une infraction pénale.

L'autorité communicante 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 s'il n'existe aucune disposition légale nationale pertinente ni aucun accord international et si la prévention d'un grave danger impose de procéder à cette communication.

La communication de données devrait systématiquement respecter les exigences de conformité 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 (STE n° 108).

Si l'autorité communicante soumet l'utilisation des données dans l'État destinataire à un certain nombre de conditions, celles-ci doivent être respectées.

Exemple :
l'État destinataire qui souhaite transmettre ces données à un autre destinataire demande au préalable à l'État communiquant l'autorisation de le faire.

La transmission à un autre destinataire des données communiquées devrait uniquement être autorisée 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. La transmission à un autre destinataire des données communiquées ne devrait pas être autorisée à des fins de police d'ordre général.

5.5.i. Demandes de communication

Sous réserve des dispositions spécifiques de la législation nationale ou d'accords internationaux, les demandes de communication de données devraient contenir des indications sur l'organe ou la personne dont elles émanent ainsi que sur leur objet et leur motif.

Le *principe 5.5* précise les dispositions qui régissent les différentes formes de communication précitées. Il s'agit notamment du Règlement d'Interpol sur le traitement des données, 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).

Ce principe vise à garantir que toute communication de données soit justifiée. Cela concerne les échanges au sein d'un pays ou avec un partenaire international. La demande doit comporter des indications précises sur son auteur et mentionner les motifs et la finalité de cette communication de données.

5.5.ii. Conditions de la communication

La qualité des données devrait, autant que possible, être vérifiée au plus tard avant leur communication. Dans toute communication de données et dans la mesure du possible, les décisions juridictionnelles ainsi que les décisions de ne pas poursuivre devraient être mentionnées et les données fondées sur des opinions ou des appréciations personnelles être vérifiées à la source avant d'être communiquées ; leur degré de fiabilité ou d'exactitude devrait être indiqué.

S'il s'avère que les données ne sont plus exactes et à jour, elles ne devraient pas être communiquées ; si des données périmées ou inexactes ont été communiquées, l'organe expéditeur devrait autant que possible informer de leur non-conformité tous les organes destinataires auxquels les données ont été transmises.

La formule « autant que possible » signifie que les conditions fixées dans cette partie du principe devraient être appliquées lorsque cela est faisable. Il est admis que la police ne soit pas systématiquement informée des décisions de justice.

Cette partie du principe présente une certaine souplesse, car on admet que les divers États membres procèdent à ces vérifications à des moments différents. C'est la raison pour laquelle la qualité des données peut être vérifiée jusqu'au moment de leur communication.

5.5.iii. Garantie concernant la communication

Les données communiquées à d'autres organes publics, à des personnes privées ou à des autorités étrangères ne devraient être utilisées à d'autres fins que celles spécifiées dans la demande de communication.

Toute utilisation à d'autres fins devrait être subordonnée à l'accord de l'organe expéditeur, sans préjudice des dispositions des paragraphes 5.2 à 5.4.

Toute donnée communiquée hors du cadre de la police nationale ne devrait pas être utilisée à d'autres fins que celles pour lesquelles elle a été communiquée ou reçue. La seule exception à ce principe est admise lorsque l'autorité expéditrice donne son accord pour une autre utilisation et lorsque cette autre utilisation est conforme à un ou plusieurs critères énoncés aux principes 5.2 à 5.4.

5.6. Mise en relation des fichiers et accès direct (accès en ligne)

La mise en relation de fichiers avec d'autres fichiers utilisés à des fins différentes est soumise à l'une des conditions suivantes :
a. l'octroi d'une autorisation par l'organe de contrôle aux fins d'une enquête sur un délit particulier, ou
b. la conformité à une disposition légale claire.

L'accès direct (accès en ligne) à un fichier ne devrait être admis que s'il est conforme à la législation interne qui devrait tenir compte des principes 3 à 6.

Ce principe concerne les situations particulières dans lesquelles la police peut chercher à collecter des données en coordonnant ses informations avec celles d'autres détenteurs de données.

Exemple :

la police peut mettre ses fichiers en relation avec des fichiers utilisés à des fins différentes, par exemple les fichiers détenus par d'autres organes publics ou des organismes privés. Elle peut agir ainsi dans le cadre d'une enquête judiciaire en cours ou pour déterminer des tendances thématiques dans un certain type d'infraction.

Pour être légale, cette démarche doit être autorisée et être prévue par la législation.

Si la police a directement accès aux fichiers d'autres services répressifs ou non répressifs, elle doit uniquement y accéder et utiliser les données consultées dans le respect de la législation nationale, qui doit être conforme aux principes fondamentaux de la protection des données.

Principe 6 – Publicité, droit d'accès aux fichiers de police, droit de rectification et droit de recours

6.1. L'autorité de contrôle devrait prendre des mesures afin de s'assurer que le public est informé de l'existence des fichiers faisant l'objet d'une notification ainsi que de ses droits vis-à-vis de ces fichiers. La mise en œuvre de ce principe devrait tenir compte de la spécificité des fichiers ad hoc, en particulier de la nécessité d'éviter que l'accomplissement d'une tâche légale des organes de police ne soit entravé gravement.

L'organe responsable des données doit veiller à ce que tout fichier pertinent soit notifié au public, accompagné des conditions particulières dont il est assorti, comme le classement par catégorie des données et les conditions d'enregistrement et de traitement. L'APD peut vérifier que les informations nécessaires sont rendues publiques.

Les informations fournies doivent respecter un juste équilibre entre tous les intérêts concernés et tenir compte de la nature particulière des fichiers ad hoc ou provisoires et des autres fichiers particulièrement sensibles, comme les fichiers de renseignement en matière pénale, afin d'éviter de porter gravement préjudice à la police dans l'exercice de ses fonctions.

Il importe que les informations soient données aux citoyens pour qu'ils aient connaissance de ces éléments, pour qu'ils soient informés de leurs droits et pour qu'ils bénéficient d'instructions claires sur l'exercice de leurs droits à l'égard de ces fichiers. Les informations fournies devraient également préciser dans quelles conditions les droits des intéressés peuvent faire l'objet d'exceptions et comment déposer un recours contre une décision prise par l'organe responsable des données à la suite d'une demande.

Les sites internet peuvent jouer un rôle d'information du public, qui ne doit pas être exclusif et peut être assumé par d'autres médias. Il est recommandé, en guise de bonnes pratiques, de mettre des modèles de lettres à la disposition des personnes qui souhaitent exercer leurs droits au sujet des données. Ces modèles pourraient être fournis par les mêmes sites internet que ceux qui assurent la publicité de l'information.

L'organe responsable des données doit veiller à fournir suffisamment d'informations au public sur son site internet ou par tout autre moyen adéquat.

Il appartient au ministère compétent de faire connaître la protection des données et les droits des intéressés dans le cadre d'une campagne publique de sensibilisation.

6.2. La personne concernée devrait pouvoir obtenir l'accès à un fichier de police à des intervalles raisonnables et sans délais excessifs conformément aux modalités prévues par le droit interne.

L'accès aux données est un droit fondamental reconnu à tout individu à l'égard des données à caractère personnel qui le concernent. Le droit interne peut prévoir un droit d'accès direct ou indirect.

S'il s'agit d'un accès direct, l'intéressé peut le demander à l'organe responsable des données. Ce dernier apprécie la demande et les éventuelles exceptions applicables, puis répond directement à l'intéressé. Lorsque le droit d'accès prévu est indirect, l'intéressé peut adresser sa demande à l'APD, qui effectue la demande en son nom et procède à la vérification de la disponibilité et de la légalité des données à caractère personnel de l'intéressé. Elle répond ensuite elle-même à l'intéressé.

La personne concernée devrait pouvoir faire cette demande d'accès gratuitement et à intervalles réguliers. L'organe responsable des données apprécie la demande et répond à l'intéressé dans le délai raisonnable prévu par le droit interne.

Il convient que les dispositions en vigueur prévoient le moyen de confirmer l'identité de l'intéressé avant toute autorisation d'accès à des données, y compris s'il délègue à un tiers la faculté d'exercer ses droits.

6.3. La personne concernée devrait pouvoir obtenir, le cas échéant, la rectification des données la concernant, contenues dans un fichier.

Les données à caractère personnel que l'exercice du droit d'accès a révélées inexactes ou qui sont apparues excessives, inexactes ou non pertinentes en application de l'un des autres principes contenus dans cette recommandation devraient être effacées ou corrigées ou bien faire l'objet d'une déclaration rectificative ajoutée au fichier.

De telles mesures d'effacement ou de rectification devraient s'étendre, dans la mesure du possible, à tous les documents annexés au fichier de police et, si elles ne sont pas exécutées immédiatement, elles devraient l'être, au plus tard, lors de l'enregistrement ou de la communication de données suivant.

Le droit reconnu à l'intéressé de pouvoir modifier toute donnée inexacte détenue à son sujet est un droit essentiel. Si l'intéressé découvre des données inexactes, excessives ou non pertinentes, il a 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.

Exemple : si une personne A fait une déclaration au sujet d'une personne B, en 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. Au lieu de supprimer la déclaration dont la fausseté a été démontrée, ils peuvent ajouter au fichier concerné une déclaration rectificative claire.

Si les données à corriger ou à supprimer ont été communiquées à des tiers, il importe que les autorités compétentes informent ces derniers des modifications à apporter.

6.4. L'exercice des droits d'accès, de rectification ou d'effacement ne saurait faire l'objet d'une restriction que dans la mesure où une telle restriction 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.

Les restrictions imposées à l'intéressé pour accéder aux données qui le concernent ou pour les rectifier devraient uniquement être prévues si cet accès ou cette rectification nuit aux attributions légales de la police, à la protection de l'intéressé, aux droits et libertés d'autrui ou à la protection de la sécurité nationale.

La police peut juger nécessaire de ne pas communiquer d'informations sur le traitement des données à caractère personnel si, par exemple, elles concernent une enquête en cours. La divulgation de telles données pourrait compromettre une enquête et devrait donc être exclue pendant toute la durée de cette enquête.

Exemple :
si la divulgation d'une information risque de mettre gravement en danger la sécurité d'un témoin ou d'un informateur, il convient de l'exclure pour ce motif.

Il importe que les restrictions imposées à la communication de données s'appliquent uniquement dans la mesure où elles sont nécessaires et qu'elles fassent l'objet d'une interprétation étroite. Chaque demande de l'intéressé doit être évaluée soigneusement, au cas par cas.

Dans l'intérêt de la personne concernée, une communication écrite peut être exclue par la loi, dans des cas d'espèce.

La personne concernée peut être amenée à fournir un extrait de son casier judiciaire à un futur employeur. La fourniture d'une copie ou d'une communication écrite peut ne pas être conforme à l'intérêt de la personne concernée ; dans ce cas, le droit interne peut autoriser la communication orale du contenu demandé.

6.5. Un refus ou une restriction de ces droits devraient être motivés par écrit. La communication de la motivation ne pourrait être refusée que dans la mesure où cela serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection des droits et libertés d'autrui.

Tout refus de donner suite à une demande de l'intéressé devrait être communiqué par écrit et indiquer clairement les raisons de cette décision, qui pourront être vérifiées par une autorité indépendante ou un juge. Il peut arriver que le fait de communiquer les motifs d'un refus présent un risque pour la police, l'intéressé 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.

6.6. Au cas où l'accès serait refusé, la personne concernée devrait disposer d'un recours auprès de l'autorité de contrôle ou d'un autre organe indépendant qui s'assurera que le refus est bien fondé.

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

Lorsque l'intéressé n'est pas satisfait de la réponse qui lui a été donnée, il importe qu'il puisse saisir d'un recours une juridiction pour que celle-ci vérifie le bien-fondé du refus. L'autorité de contrôle devrait disposer de pouvoirs suffisants pour examiner le fichier de police concerné et recevoir l'appréciation de la demande d'accès.

L'issue de cet examen ou du recours peut varier en fonction de la législation nationale, surtout lorsqu'il existe un droit d'accès direct ou indirect. Il peut arriver que l'autorité de contrôle ne soit pas tenue de communiquer les données à l'intéressé, même si rien ne justifie de lui en refuser l'accès. Dans ce cas, l'intéressé devrait être informé du fait que le

fichier de police a fait l'objet d'une vérification et que son contenu est conforme. À défaut, l'autorité de contrôle peut décider de communiquer les données du fichier à l'intéressé. En outre, la juridiction compétente peut avoir le pouvoir d'ordonner l'accès aux données du fichier, leur rectification ou leur suppression.

Principe 7 - Durée de conservation et mise à jour des données

7.1. Des mesures devraient être prises pour que les données à caractère personnel conservées à des fins de police soient effacées si elles ne sont plus nécessaires aux fins pour lesquelles elles avaient été enregistrées. A cette fin, il convient notamment de prendre en considération les critères suivants : nécessité de garder des données à la lumière des conclusions d'une enquête pour un cas donné ; prononcé d'une décision définitive et notamment acquittement ; réhabilitation ; prescription ; amnistie ; âge de la personne concernée ; catégories particulières de données.

7.2. Des règles destinées à fixer des périodes de conservation pour les différentes catégories de données à caractère personnel ainsi que des contrôles périodiques sur leur qualité devraient être établis en accord avec l'autorité de contrôle ou conformément au droit interne.

Il convient de prévoir des dispositions applicables à l'enregistrement et à la conservation des données. Les fichiers de police devraient être réexaminés périodiquement, afin de veiller à ce que les données qui ne sont plus nécessaires soient supprimées.

Il importe de vérifier régulièrement la qualité des données au regard de ces dispositions. Ces dernières peuvent être prévues par le droit interne ou dans le cadre d'un accord passé avec l'APD.

Si ces dispositions sont établies par la police, il convient que cette dernière consulte l'autorité de contrôle pour s'assurer qu'elles sont conformes à leur finalité.

Les critères susmentionnés doivent être pris en considération pour déterminer si les données sont toujours nécessaires pour prévenir, déceler ou enquêter sur une infraction pénale. Cela vaut également pour la conservation des données à des fins de vérification.

Il est recommandé de mettre en place un mécanisme automatique de suppression des fichiers conformément à la date limite prévue pour la conservation des données, ainsi qu'un avertissement automatique suffisamment précoce de la prochaine extinction du délai de conservation.

Il convient de mettre en place un journal des vérifications et contrôles effectués.

Principe 8 - Sécurité des données

L'organe responsable devrait prendre toutes les mesures nécessaires pour garantir aux données la sécurité physique et logique adéquate, et pour empêcher l'accès ou la communication non autorisés ou l'altération. A cette fin, il faudrait tenir compte des différents contenus et caractéristiques des fichiers.

La sécurité des informations est essentielle à la protection des données. Un ensemble de procédures destinées à garantir l'intégrité de toutes les formes d'information 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 à un niveau prédéterminé.

Le niveau de protection conférée à une base de données et/ou à un système de 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 convient de procéder au cryptage systématique des informations sensibles. Un régime de vérification peut être mis en œuvre pour vérifier l'adéquation du niveau de sécurité.

Il est conseillé aux services de police de procéder à une Évaluation de l'impact sur le respect de la vie privée (et sur la protection des données), afin d'évaluer les risques que présentent, pour la vie privée de l'intéressé, la collecte, l'utilisation et la communication des informations. Elle permettra de recenser les risques et d'élaborer des solutions pour remédier efficacement aux défaillances constatées.

Il convient d'utiliser un Système de gestion de l'identité et de l'accès pour gérer l'accès des agents 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. L'exigence d'un Système de gestion de l'identité et de l'accès est essentielle pour garantir un accès sécurisé et adéquat aux données.

L'organe responsable 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 moyens utilisés pour les 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 ;

Le respect de la vie privée dès l'élaboration
Le respect de 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 informatiques, afin de minimiser le risque de violation des données. Cette méthode, le respect de la vie privée dès l'élaboration, favorise dès le départ 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. Le respect de la vie privée dès l'élaboration exige 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.

Il importe que l'organe responsable des données veille à ce que la protection de la vie privée et des données soit solidement 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
Ce terme désigne une série de technologies différentes, qui visent à protéger les données à caractère personnel sensibles des systèmes informatiques. Les technologies de

renforcement de la protection de la vie privée permettent de prévenir le traitement excessif des données à caractère personnel, sans amoindrir la fonctionnalité 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 :

FIU.NET - Cellules de renseignement financier (CRF) de l'UE, a été lancé en 2013 pour ajouter au système d'échange d'informations existant les technologies de renforcement de la protection de la vie privée, au moyen du réseau informatique décentralisé FIU.NET.

FIU.NET sert à lutter contre le blanchiment de capitaux et le financement du terrorisme. Le traitement des données par FIU.NET exclut les demandes inutiles, améliore leur opportunité et renforce la protection de la vie privée au moyen d'une analyse autonome et anonyme des données.
Les technologies de renforcement de la protection de la vie privée utilisées permettent aux CRF connectées de rapprocher leurs données de celles des autres CRF, afin de vérifier si ces dernières disposent d'informations sur un individu précis dans leurs bases de données, de procéder à des analyses conjointes pour déceler des relations et des réseaux et pour déterminer les tendances et les risques des diverses sources de données.
Les principes essentiels de ces technologies sont l'autonomie et la décentralisation : ils garantissent le contrôle des informations à leurs détenteurs et une gouvernance des données sur les sources d'information ainsi connectées.

L'informatique dématérialisée (Cloud Computing)

L'informatique dématérialisée utilise des réseaux pour connecter les dispositifs des utilisateurs, comme les ordinateurs ou les smart phones, à des ressources centralisées dans un centre de données. L'accès aux espaces de stockage en ligne de données est possible n'importe où, ce qui permet aux travailleurs mobiles d'accéder à leur système à la demande.

L'informatique dématérialisée transforme le mode d'utilisation des technologies de l'information et des communications (TIC). Il est difficile de définir et d'assurer la protection et la sécurité des données de la même manière dans les différents espaces de stockage en ligne. Cela tient au fait qu'ils reposent, dans les divers pays du monde, sur des systèmes juridiques et des niveaux de protection des données différents. Il est par conséquent fréquent que les organisations ne mesurent pas les risques de l'informatique dématérialisée, ce qui impose de procéder au cryptage des données avant de recourir à ces services.

Il est essentiel de rédiger des contrats efficaces, qui permettent de revoir régulièrement les dispositions contractuelles, afin d'assurer à l'organisation le niveau de protection dont elle a besoin.