Groupe de travail «Article 29» sur la protection des données

Groupe de travail «Police et justice»

02356/09/FR
WP 168

L'avenir de la protection de la vie privée

Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel

Adoptée le 1er décembre 2009

Résumé

Le 9 juillet 2009, la Commission a lancé une consultation sur le cadre juridique du droit fondamental à la protection des données à caractère personnel. Dans le cadre de sa consultation, la Commission appelle à la communication d'avis sur les nouveaux défis de la protection des données à caractère personnel, notamment au regard des nouvelles technologies et de la mondialisation. Elle entend ainsi recueillir des éléments de réflexion pour déterminer si le cadre juridique actuel répond aux besoins et quelles mesures devraient être prises à l'avenir pour relever les défis identifiés. Le présent document expose la réponse conjointe à cette consultation du groupe de travail Article 29 (ci-après dénommé «groupe de travail 29») et du groupe de travail «Police et justice».

Le message central de cette contribution est que les principes essentiels de la protection des données restent valables en dépit des nouvelles technologies et de la mondialisation. Il est possible d'améliorer le niveau de protection des données dans l'UE grâce à une meilleure application des principes actuels de protection des données dans la pratique. Cela ne signifie pas pour autant qu'aucun changement législatif n'est nécessaire. Au contraire, il est utile de saisir cette occasion pour:

- préciser les modalités d'application de certaines règles et principes clés en matière de protection des données (tels que le consentement et la transparence);
- moderniser le cadre actuel, par l'ajout de nouveaux principes (tels que la «prise en compte du respect de la vie privée dès la conception» et la «responsabilité»);
- renforcer l'efficacité du système par la modernisation des dispositions de la directive 95/46/CE (par exemple en limitant la charge administrative);
- intégrer les principes fondamentaux de la protection des données dans un cadre juridique global, qui s'applique également à la coopération policière et judicaire en matière pénale.

Dans le chapitre 1, une introduction présente brièvement l'historique et le contexte de la protection des données dans l'UE.

Le chapitre 2 propose l'introduction d'un cadre juridique global. Il reconnaît la nécessité d'élaborer des règles spécifiques (*leges speciales*), à condition que celles-ci s'inscrivent dans un cadre global et soient conformes aux principes essentiels. Les garanties et principes essentiels de la protection des données devraient s'appliquer au traitement des données dans tous les secteurs.

Les chapitres 3 et 4 examinent les principaux défis en matière de protection des données.

Le chapitre 3 sur la mondialisation expose qu'en vertu du droit de l'Union, la protection des données est un droit fondamental. L'UE et ses États membres devraient garantir à tous ce droit fondamental, dans la mesure de leurs compétences. Chaque individu devrait pouvoir réclamer la protection de ses données, même lorsqu'elles font l'objet d'un traitement à l'extérieur de l'UE. C'est pourquoi il est demandé à la Commission de promouvoir la poursuite de l'élaboration de normes internationales globales en matière de protection des données à caractère personnel. En outre, il est nécessaire de repenser le processus d'évaluation du caractère adéquat de la protection. Par ailleurs, les accords internationaux peuvent constituer des instruments pertinents pour la protection des données à caractère personnel, à l'échelon mondial, et le futur cadre juridique pourrait prévoir les conditions des accords conclus avec des pays tiers. Le traitement des données

en dehors de l'UE peut également être protégé par des règles d'entreprise contraignantes. Il convient de renforcer davantage la disposition sur les règles d'entreprise contraignantes et de l'intégrer dans le nouveau cadre juridique. En ce qui concerne le droit applicable, le groupe de travail 29 envisage de rendre son avis à la Commission au cours de l'année prochaine.

Selon le chapitre 4 consacré aux évolutions technologiques, la directive 95/46/CE a bien résisté aux nombreux progrès technologiques grâce à ses principes et concepts solides et neutres sur le plan technologique. Ces derniers demeurent tout aussi pertinents, valables et applicables dans le monde connecté actuel. Les avancées technologiques ont accru les risques liés à la protection de la vie privée et des données des personnes physiques. Pour compenser ces risques, le principe de la «prise en compte du respect de la vie privée dès la conception» devrait être introduit dans le nouveau cadre: la protection de la vie privée et des données devrait être intégrée dès la conception des technologies de l'information et de la communication. L'application d'un tel principe soulignerait la nécessité de mettre en œuvre des technologies visant à améliorer la protection de la vie privée, un paramétrage par défaut favorable à la prise en compte du respect de la vie privée et les outils indispensables aux utilisateurs pour mieux protéger leurs données à caractère personnel. Par conséquent, ce principe de «prise en compte du respect de la vie privée dès la conception» devrait non seulement être contraignant pour les responsables du traitement des données mais également pour les concepteurs et producteurs de technologies. Qui plus est, il conviendrait d'adopter, le cas échéant, des règlements applicables dans des circonstances technologiques spécifiques, prévoyant la prise en compte des principes de protection des données et de respect de la vie privée.

Selon les chapitres 5, 6 et 7, les principaux défis en matière de protection des données nécessitent un renforcement du rôle des différents acteurs.

L'évolution du comportement et du rôle des personnes concernées, ainsi que l'expérience acquise grâce à la directive 95/46/CE imposent d'accorder aux personnes une place plus importante en ce qui concerne la protection des données. Le chapitre 5 expose les propositions visant à donner à la personne les moyens de jouer un rôle plus actif. Pour atteindre cet objectif, il est notamment nécessaire d'améliorer les voies de recours. Les personnes devraient disposer de moyens plus nombreux pour exercer et faire valoir leurs droits, notamment par l'introduction de procédures de recours collectif, de procédures de plainte et d'autres modes de règlement des conflits plus accessibles, plus efficaces et moins coûteux. En outre, le nouveau cadre devrait prévoir des solutions alternatives permettant une plus grande transparence et l'introduction d'une notification générale en cas de violation de la vie privée. Le «consentement» est un motif de traitement important qui pourrait, dans certaines circonstances, donner plus de pouvoir à la personne concernée. Néanmoins, à l'heure actuelle, on prétend souvent à tort qu'il est le motif applicable, étant donné que les conditions du consentement ne sont pas entièrement réunies. En conséquence, le nouveau cadre devrait préciser les conditions du «consentement». De plus, il convient de favoriser l'harmonisation, car l'absence d'harmonisation des législations nationales transposant la directive 95/46/CE empêche de donner plus de pouvoir aux personnes concernées. Enfin, le rôle des personnes concernées sur l'internet est un sujet de préoccupation qui doit être encore précisé dans la perspective du nouveau cadre juridique. En tout état de cause, quiconque propose des services à une personne physique devrait être tenu de fournir certaines garanties en matière de sécurité et, le cas échéant, de confidentialité des informations téléchargées par les utilisateurs, que son client soit ou non un responsable du traitement des données.

Le chapitre 6 vise à renforcer la responsabilité des autorités chargées du traitement des données. La protection des données devrait en premier lieu être ancrée dans les organisations. Elle devrait faire partie intégrante de leurs valeurs et pratiques communes, et il convient d'en attribuer expressément la responsabilité. Cette démarche aidera également les autorités chargées de la protection des données dans leurs missions de surveillance et de lutte contre les infractions, rendant ainsi la protection de la vie privée plus efficace. Les responsables du traitement des données doivent prendre un certain nombre de mesures proactives et réactives, précisées dans ce chapitre. En outre, il serait judicieux d'introduire le principe de responsabilité dans le cadre global, afin de contraindre les responsables du traitement des données à prendre les mesures nécessaires pour veiller à ce que les principes et obligations essentiels de la directive actuelle soient respectés lors du traitement des données à caractère personnel, mais également pour disposer des mécanismes internes nécessaires démontrant le respect de ces exigences par les parties prenantes extérieures, y compris les autorités chargées de la protection des données. Les notifications d'opérations de traitement des données aux autorités nationales de protection pourraient être simplifiées, voire réduites. Il conviendrait d'examiner si, et dans quelle mesure, la notification pourrait être limitée aux situations dans lesquelles le risque pour la protection de la vie privée est élevé, ce qui permettrait aux autorités chargées de la protection des données d'être plus sélectives et de concentrer leurs efforts sur ces cas, mais également de déterminer les modalités de simplification de cette notification.

Le chapitre 7, point a, envisage un rôle accru et plus précis pour les autorités nationales chargées de la protection des données. À l'heure actuelle, les États membres ont des avis très divergents en ce qui concerne, notamment, le rôle, les ressources et les pouvoirs des autorités chargées de la protection des données. Les nouveaux défis auxquels la protection des données est confrontée réclament desdites autorités un contrôle renforcé, plus homogène et efficace. En conséquence, le nouveau cadre devrait garantir l'uniformité des normes en ce qui concerne l'indépendance, les pouvoirs réels, le rôle consultatif de ces autorités dans le processus législatif et leur capacité à fixer leur propre programme de travail, notamment la définition des priorités en matière de traitement des plaintes. De telles normes devraient être adoptées à haut niveau par des instances qui font autorité.

Le chapitre 7, point b, décrit comment la coopération entre les autorités chargées de la protection des données devrait être améliorée. Les autorités européennes chargées de la protection des données sont réunies au sein du groupe de travail 29. La première priorité devrait être de veiller à ce que toutes les questions liées au traitement des données à caractère personnel, en particulier dans le domaine de la coopération policière et judiciaire en matière pénale, fassent partie intégrante des activités du groupe de travail 29 actuel. En outre, les méthodes de travail du groupe devraient encore être améliorées. Il conviendrait, le cas échéant, de souligner l'engagement renouvelé des membres du groupe de travail à mettre en œuvre les avis de ce dernier, à l'échelon national. Les relations entre le groupe de travail 29 et la Commission, qui en assure le secrétariat, peuvent encore être améliorées par la description du rôle essentiel de chacun dans un protocole d'accord. Le groupe de travail 29 lancera en 2010 une consultation avec la Commission sur ce protocole.

Enfin, le chapitre 8 aborde les défis de la protection des données dans le domaine particulièrement préoccupant de la police et de la lutte contre la criminalité. Cette

question, dans le contexte de l'UE, a évolué depuis l'entrée en vigueur du traité de Lisbonne. La décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale peut être perçue comme un premier pas vers la création d'un cadre général relevant de l'ex-troisième pilier, bien qu'elle reste largement incomplète. Ces dernières années, le nombre de données à caractère personnel conservées et échangées dans le cadre d'activités policières et judiciaires a considérablement augmenté, en raison des besoins croissants d'utilisation de ces informations pour combattre les nouvelles menaces du terrorisme et de la criminalité organisée, et sous l'effet des évolutions technologiques. Dans ce contexte, les défis de la protection des données sont immenses et devraient être traités dans le futur cadre juridique. Le chapitre 8 détaille les conditions d'élaboration des lois et des politiques en matière de protection des données dans le domaine de la police et de la lutte contre la criminalité, à savoir un échange d'informations basé sur une stratégie cohérente; une évaluation périodique des mesures et instruments juridiques actuels et de leur application; la transparence et la prise en compte de l'accès et des droits de rectification dans un contexte transfrontalier; la transparence et le contrôle démocratique du processus législatif; l'architecture des systèmes de stockage et d'échange des données à caractère personnel; un cadre clair pour les relations avec les États tiers, qui soit contraignant pour toutes les parties et fondé sur la notion d'évaluation du caractère adéquat de la protection; une attention particulière accordée aux systèmes d'information à grande échelle dans l'UE; une prise en compte adaptée du contrôle indépendant, du contrôle judiciaire et des voies de recours, ainsi qu'une coopération renforcée entre les autorités chargées de la protection des données.

1. Introduction

La consultation

1. Le 9 juillet 2009, la Commission a lancé une consultation sur le cadre juridique du droit fondamental à la protection des données à caractère personnel. Dans le cadre de sa consultation, la Commission appelle à la communication d'avis sur les nouveaux défis de la protection des données à caractère personnel, notamment au regard des nouvelles technologies et de la mondialisation. Elle entend ainsi recueillir des éléments de réflexion pour déterminer si le cadre juridique actuel répond aux besoins et quelles mesures devraient être prises à l'avenir pour relever les défis identifiés.

2. Le présent document expose la réponse conjointe à cette consultation du groupe de travail Article 29 (ci-après dénommé «groupe de travail 29») et du groupe de travail «Police et justice».

Historique et contexte

3. La convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)[1] peut être considérée comme le premier cadre juridique européen du droit fondamental à la protection des données à caractère personnel. Le droit à la protection des données est étroitement lié, mais n'est pas identique, au droit à la vie privée visé à l'article 8 de la Convention européenne des droits de l'homme. Il est reconnu comme un droit fondamental autonome par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

[1] STE n° 108, 28.1.1981.

4. Les principes de la Convention 108 ont été précisés dans la directive 95/46/CE[2] qui est la pierre angulaire de la législation sur la protection des données dans l'UE. L'efficacité (future) de la directive est le principal objet de la consultation de la Commission. Les autres instruments législatifs de l'UE en matière de protection des données sont le règlement n° (CE) 45/2001[3] applicable au traitement des données par les institutions et les organismes de l'UE, la directive 2002/58/CE[4] sur la vie privée et les communications électroniques, et la décision-cadre 2008/977/JAI[5] relative à la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale.

5. Le traité de Lisbonne accorde à la protection des données une importance considérable. Non seulement la Charte des droits fondamentaux de l'Union européenne est devenue contraignante, mais l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), qui a été ajouté, constitue une nouvelle base juridique pour la protection des données applicable à tous les traitements de données à caractère personnel, dans les secteurs public et privé, y compris dans le domaine de la coopération policière et judiciaire et dans le cadre de la politique étrangère et de sécurité commune. L'article 16 renforce la protection des données.

6. Dans ce contexte, il convient de mentionner également le «Programme de Stockholm», programme pluriannuel de l'Union européenne qui accorde une grande importance à la protection des données dans un espace de liberté, de sécurité et de justice au service de la protection du citoyen.[6]

Message central

7. La consultation de la Commission arrive à un moment fort opportun en raison des importants nouveaux défis posés par les nouvelles technologies et la mondialisation, mais également dans la perspective du traité de Lisbonne.

8. Le message central est que les principes fondamentaux de la protection des données restent valables malgré ces défis importants. Le niveau de protection des données dans l'UE peut être amélioré grâce à une meilleure application des principes actuels de protection des données. Cela ne signifie pas pour autant qu'aucun changement législatif n'est nécessaire. Au contraire, il est utile de saisir cette occasion pour:

---

2 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31.

3 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO L 8 du 12.1.2001, p. 1.

4 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37; telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009.

5 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60, à transposer dans la législation nationale avant le 27 novembre 2010.

6 Le Programme de Stockholm: un espace européen ouvert et sûr, au service du citoyen et de sa protection, devant être approuvé par le Conseil européen en décembre 2009.

- préciser les modalités d'application de certaines règles et principes clés en matière de protection des données (tels que le consentement et la transparence);
- actualiser le cadre par l'ajout de nouveaux principes (tels que la «prise en compte du respect de la vie privée dès la conception» et la «responsabilité»);
- renforcer l'efficacité du système par la modernisation des dispositions de la directive 95/46/CE (par exemple en limitant la charge administrative);
- intégrer les principes fondamentaux de la protection des données dans un cadre juridique global, qui s'applique également à la coopération policière et judiciaire en matière pénale.

2. Un cadre global unique

Le cadre juridique actuel

9. La protection des données, telle qu'introduite dans le cadre juridique de l'Union européenne, relève du marché intérieur. La directive 95/46/CE est fondée sur l'article 95 CE. Son objectif est double. En effet, la création et le fonctionnement du marché intérieur nécessitent que les données à caractère personnel puissent circuler librement entre les États membres et que, dans le même temps, un niveau élevé de protection des droits fondamentaux des personnes soit garanti.

10. La directive 95/46/CE est conçue comme un cadre juridique général susceptible d'être complété par des régimes spécifiques de protection des données, pour des secteurs particuliers. Jusqu'à présent, un seul régime spécifique a été adopté: celui relatif à la protection de la vie privée dans le secteur des communications électroniques (actuellement la directive 2002/58/CE). En outre, plusieurs instruments législatifs sectoriels prévoient également des règles spécifiques en matière de traitement des données à caractère personnel[7] (blanchiment d'argent, législation douanière ou systèmes VIS, EURODAC ou SIS II).

11. Le recours à l'article 95 CE a eu une incidence sur le champ d'application de la directive 95/46/CE. Si la directive a été conçue comme un cadre général pour la protection des données et fonctionne en tant que tel à bien des égards, elle ne concerne ni le traitement par les institutions de l'UE, ni les opérations de traitement qui ne relèvent pas de l'ex-premier pilier (mais principalement de l'ex-troisième pilier). En ce qui concerne le traitement par les institutions de l'UE (dans la mesure où elles relèvent de l'ex-premier pilier), le règlement n° 45/2001, qui est en grande partie similaire à la directive 95/46/CE, a été adopté. La situation actuelle, au titre de l'ex-troisième pilier, peut être décrite comme un conglomérat de régimes de protection des données applicables dans diverses situations. Si certaines différences entre ces régimes tiennent à la spécificité du secteur concerné, d'autres sont simplement le fruit d'une histoire législative différent. La décision-cadre 2008/977/JAI peut être considérée comme un premier pas vers la création d'un cadre plus général.

[7] Par exemple la directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JO L 309 du 25.11.2005, p. 15 et les différents instruments juridiques pour les systèmes d'information à grande échelle SIS, VIS et EURODAC.

12. Cette situation n'est pas satisfaisante, notamment en ce qui concerne le troisième pilier:

- il est de plus en plus admis que la protection des données est désormais une préoccupation générale de l'Union européenne qui n'est pas nécessairement liée au marché intérieur. En témoigne, par exemple, l'article 8 de la Charte des droits fondamentaux de l'Union européenne;
- ces dernières années, et assurément depuis les attentats terroristes du 11 septembre 2001 aux États-Unis, l'échange des données à caractère personnel entre les États membres fait désormais partie intégrante de la coopération policière et judiciaire, et requiert bien entendu une protection adéquate;
- l'ancienne structure en piliers ne reflète pas la réalité de la protection des données. Les données à caractère personnel sont utilisées dans des situations communes aux différents piliers, comme l'illustrent le PNR et les arrêts concernant la conservation des données rendus par la Cour de justice des Communautés européennes dans des affaires d'exploitation, aux fins de la lutte contre la criminalité, d'informations collectées initialement dans un contexte économique.

La nécessité d'un nouveau cadre

13. Les lacunes du système actuel imposent de réfléchir à «un cadre de protection des données global et cohérent, couvrant tous les domaines de compétence de l'UE»[8]. Le traité de Lisbonne prévoit une nouvelle approche horizontale de la protection des données et de la vie privée, ainsi que la base juridique nécessaire (article 16 du TFUE[9]) pour éliminer les différences et divergences actuelles qui nuisent à une protection complète, cohérente et efficace de chaque individu.

14. Les garanties et principes essentiels devraient s'appliquer au traitement des données dans tous les secteurs, de sorte à assurer une approche intégrée, mais également une protection complète, cohérente et efficace.

15. La directive 95/46/CE devrait servir de référence au cadre global qui a pour principal objectif l'efficacité et la protection efficace des personnes. Les principes actuels de la protection des données doivent être approuvés et complétés par des mesures permettant de les mettre en œuvre plus efficacement (et d'assurer une protection plus efficace des données à caractère personnel des citoyens).

16. Les principes essentiels de la protection des données devraient constituer l'épine dorsale d'un cadre global: les notions (qui/responsable de données – quoi/données à caractère personnel) et principes clés devraient être réaffirmés, en particulier les principes de licéité, d'équité, de proportionnalité, de limitation des finalités, de transparence, ainsi que les droits des personnes concernées et le contrôle

---

8 Formulation employée par la Commission dans COM (2009)262 final.

9 L'article 16 TFUE couvre non seulement le troisième pilier mais également le deuxième (politique étrangère et de sécurité commune) en ce qui concerne le traitement des données à caractère personnel par les institutions de l'UE. L'article 39 TUE prévoit une base juridique spécifique pour le traitement des données par les États membres au titre du deuxième pilier. Ces dispositions s'appliquent par exemple aux listes de terroristes établies par l'UE et les États membres, mais ne seront pas spécifiquement évoquées dans le présent chapitre.

indépendant par les autorités publiques. La refonte du cadre offre également l'occasion de clarifier la mise en œuvre de certaines notions clés telles que:

- le consentement: il convient d'éviter la confusion entre le consentement préalable («opt-in») et l'option de refus («opt-out») devrait être évitée, de même que l'utilisation du consentement dans des situations où il ne constitue pas la base juridique appropriée (voir également le chapitre 5);
- la transparence: elle est une condition préalable au traitement équitable. Il convient de préciser que la transparence ne conduit pas nécessairement au consentement. Elle est néanmoins une condition préalable à un consentement valable et à l'exercice des droits de la personne concernée (voir également le chapitre 5).

L'objectif devrait être d'améliorer la protection des données au niveau international, conformément aux principes et aux droits définis par la directive 95/46/CE, tout en maintenant le niveau actuel de protection (voir également le chapitre 3).

17. L'adoption d'un cadre global unique permettrait aussi d'actualiser utilement les règles existantes, notamment en introduisant le principe général de «prise en compte du respect de la vie privée dès la conception» dans le prolongement des règles actuelles en matière de mesures d'organisation et de sécurité technique (voir également le chapitre 4) et le principe général de responsabilité (voir également le chapitre 6).

L'architecture d'un cadre global

18. L'existence d'un cadre global unique, reposant, conformément au traité de Lisbonne, sur une base juridique unique, ne signifie pas nécessairement que toute souplesse et toute différence entre les secteurs et entre les États membres est exclue du champ d'application dudit cadre. Des règles spécifiques (*leges speciales*) pourraient le compléter et améliorer la protection, à condition qu'elles soient conformes à la notion de cadre global et respectent les principes essentiels précédemment évoqués.

19. Des règlements sectoriels et spécifiques supplémentaires pourraient être envisagés, par exemple en ce qui concerne:

- des secteurs spécifiques, tels que la santé publique, l'emploi ou les systèmes de transport intelligents;
- les outils et services liés au respect de la vie privée, tels que les certifications et les audits (voir également les chapitres 4 et 6);
- les violations de la sécurité (en complément du principe de sécurité, voir également les chapitres 5 et 6);
- la coopération policière et judiciaire, telle qu'explicitement prévue dans la déclaration 21 annexée au traité de Lisbonne (voir ci-après le chapitre 8);
- la politique en matière de sécurité nationale, telle qu'explicitement prévue dans la déclaration 20 annexée au traité de Lisbonne.

20. Des règlements nationaux supplémentaires pourraient être envisagés, compte tenu des différences culturelles et de l'organisation interne des États membres, à condition qu'ils ne nuisent pas à l'harmonisation nécessaire dans une Union européenne sans frontières intérieures.

21. Une harmonisation accrue est indispensable dans un cadre juridique clair et non équivoque, sans pour autant exclure la valeur ajoutée que peut apporter une certaine souplesse, comme le reconnaît actuellement la directive 95/46/CE, par exemple, si cette souplesse est nécessaire en raison de différences culturelles. On pourrait également laisser au législateur national la possibilité d'attribuer les responsabilités et de reconnaître les différents rôles des secteurs public et privé.

3. Mondialisation

Le contexte et le cadre juridique actuel

22. Dans le droit de l'UE, la protection des données est un droit fondamental, consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne (voir également le chapitre 1). Dans d'autres régions du monde, la nécessité de protéger les données est largement reconnue, mais pas nécessairement avec le statut d'un droit fondamental.

23. L'UE et ses États membres devraient garantir ce droit fondamental à toute personne, dans la mesure de leurs compétences. Dans un monde globalisé, cela signifie que les personnes physiques peuvent également réclamer la protection de leurs données si ces dernières font l'objet d'un traitement à l'extérieur de l'Union européenne.

24. La directive 95/46/CE répond à ce besoin de protection dans son article 4. Elle est applicable au traitement des données dans le monde entier et donc aussi à l'extérieur de l'UE[10] (a) lorsque le responsable du traitement des données est établi dans l'UE et (b) lorsqu'il est établi en dehors de l'UE mais utilise des équipements situés dans l'Union.

25. En outre, les articles 25 et 26 de la directive 95/46/CE prévoient un régime spécifique pour le transfert des données à caractère personnel vers les pays tiers. La règle fondamentale de l'article 25 autorise le transfert des données uniquement vers les pays tiers qui assurent un niveau de protection adéquat. L'article 26 prévoit un certain nombre de dérogations à cette règle. Des notions bien connues, comme les règles d'entreprise contraignantes et les clauses contractuelles types, mettent en œuvre cette disposition.

Droit applicable

26. La portée exacte de la directive 95/46/CE n'est toutefois pas suffisamment claire. On ne sait pas toujours si le droit de l'UE est applicable, quel droit national s'applique et quel(s) droit(s) s'appliquerai(en)t lorsque plusieurs établissements d'une société multinationale sont implantés dans différents États membres. L'article 4 de la directive, qui détermine les cas où celle-ci est applicable au traitement des données, laisse le champ libre à différentes interprétations.

27. En outre, certaines situations ne relèvent pas du champ d'application de la directive. C'est le cas lorsque les activités de responsables du traitement des données établis en dehors de l'UE concernent des résidents de l'UE, ce qui donne lieu à la collecte et à un traitement supplémentaire de données à caractère personnel. C'est le cas par exemple des commerçants en ligne et d'autres fournisseurs qui utilisent des publicités «couleur locale», des sites web qui ciblent directement les citoyens de

[10] Dans ce contexte, l'UE englobe également les pays de l'AELE.

l'UE (dans leur langue notamment). Si ces activités sont menées sans utiliser d'équipements installés dans l'UE, la directive 95/46/CE ne s'applique pas.

28. Le groupe de travail 29 prépare actuellement un avis sur la notion de droit applicable, qu'il envisage de rendre à la Commission européenne au cours de l'année prochaine. Cet avis pourrait comprendre de nouvelles recommandations en faveur d'un futur cadre juridique.

Les normes internationales et la résolution de Madrid

29. Il devient indispensable d'élaborer des normes globales pour la protection des données. Elles faciliteraient également la circulation transfrontalière des données qui, en raison de la mondialisation, devient la règle plutôt que l'exception. Tant que des normes globales ne seront pas mises en place, la diversité perdurera. La circulation transfrontalière des données doit être facilitée et, dans le même temps, un niveau élevé de protection des données à caractère personnel doit être assuré lorsque celles-ci font l'objet d'un transfert et d'un traitement dans des pays tiers.

30. La «résolution de Madrid», proposition conjointe de normes internationales pour la protection de la vie privée adoptée le 6 novembre 2009 par la Conférence internationale des commissaires à la protection des données et de la vie privée, mérite d'être soutenue. La proposition présente un projet de norme globale et réunit toutes les approches possibles en matière de protection des données à caractère personnel et de la vie privée, en intégrant la législation des cinq continents. Elle propose une série de principes, droits et obligations qui devraient constituer le socle de la protection des données de tout système juridique dans le monde, et démontre que des normes globales offrant un niveau adéquat de protection des données peuvent être élaborées en temps utile.

31. Il est demandé à la Commission de:

- prendre des initiatives pour renforcer le développement de normes internationales globales pour la protection des données à caractère personnel, afin de promouvoir un cadre international pour la protection des données et faciliter ainsi la circulation transfrontalière des données, tout en assurant un niveau de protection adéquat des personnes concernées. Ces initiatives devraient également examiner la faisabilité d'un cadre international contraignant;
- promouvoir, en l'absence de normes globales, le développement de la législation en matière de protection des données pour assurer un niveau de protection adéquat, et la création d'autorités indépendantes chargées de la protection des données dans les pays extérieurs à l'Union européenne. Les principes fondamentaux de la protection des données, tels qu'énoncés dans la «résolution de Madrid», devraient constituer la base universelle d'une telle législation.

Ces missions spécifiques de la Commission devraient figurer dans le futur cadre juridique.

Amélioration des décisions relatives au niveau de protection adéquat

32. Dans un environnement mondialisé, le nombre d'opérations de traitement de données à caractère personnel ne cesse de progresser. Assurer la libre circulation des

données à caractère personnel tout en garantissant le niveau de protection des droits des personnes est une exigence toujours plus forte. Il est donc nécessaire de repenser le processus d'évaluation du caractère adéquat de la protection:

- en définissant de manière plus précise les critères permettant d'atteindre le statut juridique de «niveau de protection adéquat», en tenant pleinement compte de l'approche du groupe de travail 29[11] et de diverses autres approches de la protection des données dans le monde, et notamment les droits et principes définis par la proposition conjointe de normes internationales sur la protection de la vie privée;
- en rationalisant les procédures d'analyse des régimes juridiques des pays tiers, afin de prendre davantage de décisions sur le niveau de protection adéquat.

Le futur cadre juridique devrait préciser ces questions.

Accords internationaux

33. Il a été pris bonne note des activités du groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel. Ces activités pourraient conduire à un accord transatlantique prévoyant des principes communs pour la protection de la vie privée et des données applicables à l'échange d'informations avec les États-Unis, dans le cadre de la lutte contre le terrorisme et la criminalité transnationale grave[12].

34. Les accords internationaux sont des instruments appropriés pour la protection des données à caractère personnel dans un contexte mondial, à condition que le niveau de protection offert soit au moins équivalent aux normes globales précédemment évoquées, que toute personne physique dispose d'un recours facile et efficace, notamment au niveau juridique, et que des garanties spécifiques soient fournies en ce qui concerne la finalité envisagée pour ces données à caractère personnel.

35. Si ces conditions sont remplies, l'accord transatlantique envisagé pourrait servir de modèle pour l'échange d'informations avec d'autres pays tiers et à d'autres fins. Le futur cadre juridique pourrait prévoir les conditions applicables aux accords conclus avec des pays tiers.

36. En outre, l'UE devrait encourager la coopération entre les autorités internationales de protection des données, par exemple, au niveau transatlantique. Une telle coopération permettrait de promouvoir efficacement la protection des données à l'extérieur de l'UE.

Règles d'entreprise contraignantes/responsabilité

37. Le traitement des données à l'extérieur de l'UE peut également être protégé par des règles d'entreprise contraignantes, codes de conduite internationaux pour les sociétés multinationales, qui prévoient un transfert des données au niveau mondial au sein d'une entreprise multinationale. Les règles d'entreprise contraignantes ont été introduites par le groupe de travail 29 en 2003. Les autorités chargées de la protection des données comme les multinationales les considèrent comme un moyen

[11] Voir en particulier le document de travail 12 du groupe de travail 29, intitulé «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données», adopté le 24 juillet 1998.

[12] À cet égard, le problème transatlantique concernant les recours reste à résoudre.

efficace de faciliter la circulation internationale des données tout en garantissant la protection des données à caractère personnel. Néanmoins, la directive 95/46/CE ne tient pas expressément compte de ces règles. Par conséquent, le processus d'adoption des règles d'entreprise contraignantes, qui repose sur l'article 26, paragraphe 2, de la directive 95/46/CE, requiert l'approbation de tous les États membres concernés. Dès lors, le processus d'évaluation et d'approbation des règles d'entreprise contraignantes prend beaucoup de temps. Le groupe de travail 29 n'a pas ménagé ses efforts pour promouvoir et faciliter l'utilisation et l'approbation des règles d'entreprise contraignantes dans le cadre juridique actuel. Pour aller plus loin, dix-neuf autorités chargées de la protection des données ont à ce jour convenu d'une procédure d'approbation des règles d'entreprise contraignantes, appelée «reconnaissance mutuelle».

38. Dans ce contexte, le nouveau cadre juridique devrait comprendre une disposition renforcée sur les règles d'entreprise contraignantes, pour répondre à plusieurs objectifs:

- reconnaître que les règles d'entreprise contraignantes constituent un outil pertinent capable d'offrir les garanties adéquates;
- définir les principaux éléments de contenu et de procédure de ces règles, conformément aux avis rendus par le groupe de travail 29 sur cette question.

39. En outre, de manière générale, le nouveau cadre législatif pourrait comprendre une nouvelle disposition prévoyant que les responsables du traitement des données demeureraient responsables de la protection des données à caractère personnel dont ils ont la responsabilité du traitement, même en cas de transfert de ces données à d'autres responsables établis à l'extérieur de l'UE (pour la question de la «responsabilité», voir aussi plus généralement le chapitre 6).

Conclusion

40. Ce chapitre aborde la mondialisation en tant que telle, même si, d'une manière ou d'une autre, tous les chapitres de la présente contribution traitent ce thème. On associe fréquemment la «mondialisation» à l'activité économique. Pourtant, les opérations de traitement des données à caractère personnel effectuées dans un contexte mondialisé sont toujours plus nombreuses. Si le contexte local est souvent celui dans lequel évoluent les personnes physiques, ces dernières utilisent de plus en plus l'internet, où leurs données font l'objet d'un traitement mondial. La mondialisation dépend dès lors de la technologie (chapitre 4), de la place occupée par la personne concernée (chapitre 5), du responsable du traitement des données (chapitre 6), des autorités chargées de la protection des données/du groupe de travail 29 (chapitre 7) et de la lutte contre la criminalité (chapitre 8).

4. Évolutions technologiques: la prise en compte du respect de la vie privée dès la conception, un nouveau principe

41. Les concepts de base de la directive 95/46/CE ont été élaborés dans les années 1970, à une époque où le traitement des informations se caractérisait par l'utilisation de fichiers manuels, de cartes perforées et de gros systèmes informatiques. Aujourd'hui, l'informatique est omniprésente, mondiale et connectée. Les systèmes sont de plus en plus miniaturisés et équipés de cartes réseau, de WiFi et d'autres interfaces radio.

Dans presque tous les bureaux et foyers, les utilisateurs peuvent communiquer avec le monde entier via l'internet. Les services du web 2.0 et l'informatique dématérialisée ne permettent plus de distinguer les responsables du traitement des données des sous-traitants et des personnes concernées.

42. La directive 95/46/CE a bien résisté à ces évolutions technologiques, grâce à des principes et des concepts qui sont non seulement solides mais aussi neutres sur le plan technologique. Ces principes et concepts restent tout aussi pertinents, valables et applicables dans le monde connecté actuel.

43. S'il est clair que les évolutions technologiques décrites précédemment sont généralement bénéfiques pour la société, elles n'en ont pas moins accru les risques en matière de protection de la vie privée et des données à caractère personnel. Pour compenser ces risques, le cadre juridique de protection des données devrait être complété. Premièrement, le principe de «prise en compte du respect de la vie privée dès la conception» devrait être introduit dans le nouveau cadre juridique; deuxièmement, il conviendrait d'adopter, le cas échéant, des règlements applicables à des contextes technologiques spécifiques, prévoyant la prise en compte des principes de protection des données et de la vie privée dans ces contextes.

Principe de la prise en compte du respect de la vie privée dès la conception

44. L'idée d'intégrer des garanties technologiques en matière de protection des données dans les technologies de l'information et de la communication («TIC») n'est pas entièrement nouvelle. La directive 95/46/CE contient déjà plusieurs dispositions qui prévoient expressément que les responsables du traitement des données doivent mettre en œuvre des garanties technologiques lors de la conception et l'utilisation des TIC. C'est le cas de l'article 17 qui leur impose d'appliquer des mesures techniques et d'organisation appropriées. Le considérant 46 demande que de telles mesures soient prises tant au moment de la conception du système de traitement qu'à celui de la mise en œuvre du traitement lui-même. L'article 16 instaure la confidentialité du traitement, règle reprise et complétée dans les règlements sur la sécurité informatique. Outre ces articles, les principes relatifs à la qualité des données, tels que visés à l'article 6 (traitement loyal et licite, limitation des finalités, pertinence, exactitude, durée de conservation limitée, responsabilité), s'appliquent également.

45. Si les dispositions susmentionnées de la directive contribuent à promouvoir la prise en compte du respect de la vie privée dès la conception, elles n'ont, en pratique, pas suffi à garantir l'intégration du respect de la vie privée dans les TIC. Les utilisateurs de services TIC, à savoir les entreprises, le secteur public et plus encore les personnes physiques, ne sont pas en mesure de prendre eux-mêmes les mesures de sécurité appropriées pour protéger leurs propres données à caractère personnel ou celles d'autres personnes. Par conséquent, ces services et technologies devraient être conçus avec un paramétrage par défaut favorable au respect de la vie privée.

46. Aussi le nouveau cadre juridique doit-il prévoir une disposition qui traduise les prescriptions ponctuelles actuelles en un principe plus large et cohérent de prise en compte du respect de la vie privée dès la conception. Ce principe devrait être contraignant pour les concepteurs et producteurs de technologies ainsi que pour les responsables du traitement des données chargés de l'achat et de l'utilisation des TIC.

Ils devraient avoir l'obligation de prendre en compte la protection technologique des données dès la phase de planification des procédures et des systèmes technologiques d'information. Les fournisseurs de tels systèmes ou services et les responsables du traitement des données devraient démontrer qu'ils ont pris toutes les mesures requises pour remplir ces obligations.

47. Un tel principe devrait requérir la mise en œuvre de la protection des données dans les TIC (prise en compte du respect de la vie privée dès la conception) conçues ou utilisées pour le traitement des données à caractère personnel. Il devrait impliquer que les TIC doivent non seulement assurer la sécurité mais également être conçus et développés de sorte à éviter ou à limiter la quantité de données à caractère personnel traitées. Cette approche est conforme à la jurisprudence allemande récente.[13]

48. L'application de ce principe soulignerait la nécessité de mettre en œuvre des technologies qui améliorent la protection de la vie privée, un paramétrage par défaut favorable au respect de la vie privée et des outils indispensables aux utilisateurs pour mieux protéger leurs données à caractère personnel (par exemple, les contrôles d'accès ou le cryptage). Les produits et services fournis aux tiers et aux clients particuliers (par exemple les routeurs Wifi, les réseaux sociaux et les moteurs de recherche) devraient être soumis à l'obligation d'appliquer ce principe. Quant aux autorités chargées de la protection des données, elles auraient davantage de pouvoir pour mettre en œuvre efficacement de telles mesures.

49. Ce principe devrait être défini de manière *neutre sur le plan technologique* pour qu'il puisse durer longtemps dans un contexte technologique et social en constante mutation. Il devrait également être assez *souple* pour permettre aux responsables du traitement des données et aux autorités chargées de leur protection, de le convertir, au cas par cas, en mesures concrètes garantissant la protection des données.

50. Il devrait également souligner, comme le fait l'actuel considérant 46, la nécessité d'une application *dès que possible*, «tant au moment de la conception qu'à celui de la mise en œuvre du traitement». Les garanties mises en œuvre tardivement ne sont pas cohérentes ni suffisantes au regard des exigences d'une protection efficace des droits et des libertés des personnes concernées.

51. Des normes technologiques devraient être développées et prises en compte lors de la phase d'analyse du système par des ingénieurs en logiciels et matériel informatique, de sorte à limiter les difficultés liées à la définition et à la fixation des obligations découlant du principe de prise en compte du respect de la vie privée dès la conception. De telles normes pourraient être générales ou spécifiques, en fonction des finalités et des technologies de traitement.

---

[13] Récemment, la Cour constitutionnelle allemande (arrêt du 27 février 2008 - 1 BvR 370/07; 1 BvR 595/07 –) a créé un droit constitutionnel à la confidentialité et à l'intégrité des systèmes informatiques. Les systèmes capables de créer, de traiter ou de stocker des données sensibles à caractère personnel requièrent une protection particulière. Le champ de protection du droit fondamental à la confidentialité et à l'intégrité des systèmes d'informations s'étend aux systèmes qui, seuls ou du fait de leur interconnectivité technique, peuvent contenir des données à caractère personnel sur la personne concernée, à un degré et dans une diversité tels que l'accès aux systèmes fournit des informations sur des éléments importants de la vie de cette personne ou dresse un portrait révélateur de sa personnalité. Ces systèmes sont par exemple les ordinateurs personnels et les ordinateurs portables, les téléphones portables et les agendas électroniques.

52. Les exemples suivants montrent comment la prise en compte du respect de la vie privée dès la conception peut contribuer à une meilleure protection des données:

- les identificateurs biométriques devraient être conservés dans des dispositifs contrôlés par les personnes concernées (c'est-à-dire via des cartes à puces) plutôt que dans des bases de données externes;
- les systèmes de vidéosurveillance des transports publics devraient être conçus de sorte que le visage des personnes enregistrées ne soit pas reconnaissable ou que d'autres mesures soient prises pour réduire les risques pour les personnes concernées. Bien entendu, des exceptions doivent être prévues pour des circonstances exceptionnelles, par exemple lorsque la personne est suspectée d'avoir commis une infraction pénale;
- les noms des patients et d'autres identificateurs personnels conservés dans les systèmes d'information des hôpitaux devraient être séparés des données relatives à l'état de santé et au traitement médical. Ces éléments devraient être combinées uniquement en cas de nécessité, pour des raisons médicales ou d'autres raisons valables, dans un environnement sécurisé;
- si nécessaire, une fonctionnalité devrait être intégrée pour permettre à la personne concernée d'annuler son consentement, ce qui aurait pour effet de supprimer ses données de tous les serveurs concernés (y compris les serveurs proxy et miroirs).

53. En pratique, la mise en œuvre du principe de prise en compte du respect de la vie privée dès la conception exigera l'évaluation de plusieurs éléments ou objectifs concrets. En particulier, avant de décider de la conception d'un système de traitement, de son achat et de son utilisation, les éléments/objectifs généraux suivants devraient être pris en compte:

- limitation autant que possible des données: les systèmes de traitement des données doivent être conçus et choisis en accord avec la finalité de ne collecter, traiter ou exploiter aucune donnée à caractère personnel ou une quantité aussi faible que possible de ce type de données;
- capacité de contrôle: un système informatique devrait fournir aux personnes concernées des moyens de contrôle efficaces de leurs données à caractère personnel. Les possibilités d'autorisation et de refus devraient être facilitées par les moyens technologiques;
- transparence: les développeurs et gestionnaires de systèmes informatiques doivent s'assurer que les personnes concernées sont suffisamment informées du mode opératoire des systèmes. L'accès électronique / l'accès aux informations devrait être assuré;
- systèmes conviviaux: les fonctions et dispositifs associés au respect de la vie privée devraient être conviviaux, autrement dit proposer une aide suffisante et des interfaces simples, susceptibles d'être également utilisées par des personnes peu expérimentées;
- confidentialité des données: les systèmes informatiques doivent être conçus et sécurisés de sorte que seules des entités autorisées aient accès aux données à caractère personnel;
- qualité des données: les responsables du traitement des données doivent assurer la qualité des données par des moyens techniques. Les données pertinentes devraient être accessibles, le cas échéant, à des fins licites.

- restriction d'emploi: les systèmes informatiques, affectés à différentes finalités ou fonctionnant dans un environnement multi-utilisateurs (à savoir les systèmes virtuellement connectés tels que les entrepôts de données, l'informatique dématérialisée, les identificateurs numériques), doivent garantir que les données et processus servant à différentes tâches ou finalités puissent être isolés les uns des autres de manière sécurisée.

Règlements relatifs aux contextes technologiques spécifiques

54. Le principe de la prise en compte du respect de la vie privée dès la conception peut ne pas suffire à garantir, en toutes circonstances, que les principes appropriés de protection des données technologiques sont correctement pris en compte par les TIC. Dans certains cas, une approche pragmatique plus concrète pourra être nécessaire. Pour faciliter la mise en œuvre de telles mesures, un nouveau cadre juridique devrait contenir une disposition permettant l'adoption de règlements spécifiques en cas de contexte technologique particulier, exigeant la prise en compte des principes de protection de la vie privée dans ce contexte.

55. Il n'y a là aucune nouveauté: l'article 14, paragraphe 3, de la directive relative à la vie privée et aux communications électroniques prévoit une disposition similaire: «Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel, conformément à la directive 1999/5/CE et à la décision 87/95/CEE du Conseil du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications».

56. Cette disposition faciliterait l'adoption, dans des cas particuliers, de mesures législatives spécifiques intégrant le concept de «prise en compte du respect de la vie privée dès la conception» et garantissant que les spécifications adéquates sont fournies. Cela pourrait par exemple être le cas de la technologie RFID, des réseaux sociaux, de la publicité comportementale, etc.

Conclusion

57. L'importance croissante de la protection des données lors de la création et de l'exécution de systèmes informatiques soumet les informaticiens à de nouvelles obligations. Pour cette raison, la protection des données doit impérativement être intégrée dans la formation des personnels informatiques.

58. Les principes de la protection des données technologiques et les critères concrets qui en résultent devraient servir de base à l'attribution de labels de qualité (systèmes de certification) dans le cadre d'un audit de la protection des données[14].

5. Habilitation des personnes concernées

59. Toutes les possibilités associées à la place de la personne concernée dans la directive 95/46/CE n'ont pas été exploitées. En outre, tant le comportement des citoyens que le rôle des personnes concernées au regard de la protection des données ont changé, sous l'effet, notamment, des évolutions sociologiques et des nouvelles

[14] C'est par exemple le cas avec le projet EuroPriSe.

méthodes de collecte des données (par exemple à des fins de profilage). Il arrive que les personnes concernées fassent preuve de négligence en ce qui concerne la protection de leur propre vie privée, et elles sont parfois prêtes à y renoncer pour obtenir des avantages réels ou imaginaires. Et pourtant, elles attendent toujours beaucoup des entités avec lesquelles elles sont en relation commerciale. En outre, elles jouent elles-mêmes un rôle de plus en plus actif dans le traitement des données à caractère personnel, en particulier sur l'internet.

60. L'évolution du comportement et du rôle de la personne concernée, ainsi que l'expérience acquise grâce à la directive 95/46/CE imposent d'accorder aux personnes une place plus importante dans la protection des données[15]. Il est essentiel de donner à la personne concernée les moyens de jouer un rôle plus actif.

Amélioration des voies de recours

61. Pour habiliter la personne concernée, il faut lui donner davantage de possibilités d'exercer et de faire valoir ses droits. La procédure judiciaire réservant parfois de nombreuses difficultés et comportant un risque financier, la possibilité d'une procédure de recours collectif devrait être introduite dans la directive 95/46/CE[16].

62. En outre, les responsables du traitement des données devraient prévoir des procédures de plainte plus aisément accessibles, plus efficaces et moins coûteuses (voir également le chapitre 6). Si ces procédures ne permettent pas de régler le litige entre le responsable du traitement des données et la personne concernée, cette dernière devrait avoir la possibilité de recourir à des modes alternatifs de règlement des litiges, essentiellement prévus par l'industrie[17]. Ces possibilités devraient être incluses dans le nouveau cadre législatif.

Transparence

63. La transparence est une autre condition fondamentale, car elle permet à la personne concernée d'intervenir dans le traitement des données à caractère personnel en amont de celui-ci. Avec le profilage, l'extraction de données et les évolutions technologiques qui facilitent l'échange des données à caractère personnel, il est encore plus important pour la personne concernée de savoir qui traite les données, sur quelles bases, à partir de quel lieu, à quelles fins et avec quels moyens techniques. Il est important que ces informations soient compréhensibles. Toutefois, l'obligation d'information de la personne concernée (articles 10 et 11 de la directive 95/46/CE) n'est pas toujours correctement mise en pratique. Un nouveau cadre juridique devrait prévoir des solutions alternatives, pour une plus grande transparence. Par exemple, de nouvelles modalités d'information des personnes concernées pourraient être élaborées en ce qui concerne la publicité comportementale.

---

[15] C'est notamment le cas en ce qui concerne les enfants. Au moment de prendre des décisions concernant leurs données à caractère personnel, leur intérêt supérieur doit être une considération primordiale, comme le prévoit la Convention des Nations Unies relative aux droits de l'enfant (http://www2.ohchr.org/french/law/crc.htm), d'autres instruments internationaux spécifiques et la législation nationale.

[16] Des recours collectifs existent, par exemple, en droit environnemental.

[17] Ce type de procédure ne peut bien entendu pas empêcher une personne de former un recours approprié auprès d'un tribunal ou d'une autorité chargée de la protection des données.

64. En outre, la transparence impose une information des personnes concernées en cas de violation de la vie privée susceptible de nuire à leurs données à caractère personnel ainsi qu'à leur vie privée. Elles pourraient de cette manière tenter de limiter le préjudice qu'elles ont subi (dans certains cas, les autorités devraient également être informées, voir aussi le chapitre 6). La notification générale de violation de la vie privée devrait être introduite dans le nouveau cadre juridique (voir également le chapitre 6)[18].

Consentement

65. Dans la directive, le consentement de la personne concernée constitue un motif légitime de traitement des données (articles 7 et 8 de la directive 95/46/CE). Ce consentement est et demeure un motif important de traitement, qui pourrait, dans certaines circonstances, donner plus de pouvoir à la personne concernée. Toutefois, le consentement doit être une manifestation de volonté, libre, spécifique et informée [article 2, point h), de la directive 95/46/CE].

66. Dans de nombreux cas, le consentement ne peut être accordé librement, notamment en cas de déséquilibre évident entre la personne concernée et le responsable du traitement des données (par exemple, dans le contexte du travail ou lorsque les données à caractère personnel doivent être transmises aux pouvoirs publics).

67. En outre, l'exigence selon laquelle le consentement doit être informé présuppose que la personne concernée comprenne pleinement les conséquences de sa décision de consentir à un traitement de ses données. Toutefois, la complexité des pratiques de collecte des données, des modèles commerciaux, des relations entre fournisseurs et des applications technologiques dépassent, bien souvent, la capacité ou la volonté d'une personne de décider, par un choix actif, de contrôler l'utilisation et le partage d'informations[19].

68. Dans les deux hypothèses, si le consentement constitue un motif inapproprié de traitement, il est néanmoins souvent invoqué à tort comme le motif applicable. Les évolutions technologiques invitent également à un examen attentif du consentement. En pratique, l'article 7 de la directive 95/46/CE n'est pas toujours correctement appliqué, en particulier dans le contexte de l'internet, où un consentement implicite ne conduit pas toujours à un consentement non équivoque [comme le prévoit l'article 7, point a), de la directive]. Pour permettre aux personnes concernées de s'exprimer davantage en amont du traitement de leurs données à caractère personnel, il faut que le consentement soit donné explicitement (il faut par conséquent un accord préalable) pour l'ensemble du traitement basé sur le consentement[20].

---

[18] Dans l'«Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive ″vie privée et communications électroniques")», le groupe de travail 29 a relevé une approche recommandée sur la question des notifications spécifiques de violation de la vie privée reprises dans la directive relative à la vie privée et aux communications électroniques. Les mêmes recommandations s'appliquent à l'introduction de notifications générales de violation de la vie privée.

[19] Voir «Data Protection Accountability: The essential Elements – A Document for Discussion», Centre for Information Policy Leadership, qui assure le secrétariat du projet Galway, octobre 2009, p. 4.

[20] En ce qui concerne le consentement et le consentement préalable (opt-in)/l'option de refus (opt-out), voir également le chapitre 2, où il est indiqué que la confusion entre consentement préalable et option de refus doit être évitée, de même que le recours au consentement lorsqu'il ne constitue pas la base juridique adéquate.

69. Le nouveau cadre juridique devrait prévoir cette obligation de consentement, compte tenu des observations ci-dessus.

Harmonisation

70. À l'heure actuelle, l'habilitation des personnes concernées est limitée par l'absence d'harmonisation entre les législations nationales transposant la directive 95/46/CE. Plusieurs éléments de la directive qui sont essentiels pour la place des personnes concernées, tels que la disposition sur la responsabilité et la possibilité d'introduire une demande en indemnité pour préjudice immatériel[21], n'ont pas été transposés par l'ensemble des États membres. Outre ces différences de transposition de la directive 95/46CE, son interprétation dans les États membres n'est pas toujours homogène. À l'heure où la mondialisation s'intensifie, ces différences affaiblissent de plus en plus le rôle de la personne concernée. Par conséquent, il est essentiel d'améliorer l'harmonisation (voir également le chapitre 7b), en précisant si nécessaire les dispositions législatives.

Le rôle des personnes concernées sur l'internet

71. Les personnes téléchargent de plus en plus leurs propres données à caractère personnel sur l'internet (dans le cadre de réseaux sociaux, de services informatiques dématérialisés, etc.). Néanmoins, la directive 95/46/CE ne s'applique pas à la personne qui télécharge les données «pour l'exercice d'activités exclusivement personnelles ou domestiques»[22]. On peut estimer qu'elle ne s'applique pas non plus à l'entité qui fournit le service, c'est-à-dire qui héberge et met à disposition les informations téléchargées par la personne physique (à moins que l'entité ne traite les données à ses propres fins) dans la mesure où le prestataire de services peut ne pas être considéré comme un responsable du traitement[23]. Il en résulte une absence de garanties à laquelle il faudra peut-être remédier, notamment du fait que ces situations sont de plus en plus fréquentes. Dans ces circonstances, quiconque propose des services à une personne privée devrait être tenu de fournir certaines garanties en matière de sécurité et, si nécessaire, de confidentialité des informations téléchargées par les utilisateurs, que son client soit ou non un responsable du traitement des données. En outre, il conviendrait de s'intéresser à la question de savoir si les personnes concernées devraient se voir accorder davantage de moyens pour faire valoir leurs droits sur l'internet, y compris la protection des droits de tiers dont les données à caractère personnel peuvent faire l'objet d'un traitement (par exemple sur les réseaux sociaux). De nombreuses autres questions restant encore sans réponse[24], le rôle de la personne concernée sur l'internet devrait être davantage précisé, dans la perspective d'un nouveau cadre juridique.

---

[21] Dans la plupart des cas où la personne concernée a subi un dommage, il s'agit de préjudice immatériel tel que le sentiment de ne plus pouvoir évoluer librement dans les secteurs public et privé sans être observé. Ce problème est encore plus vif dans l'actuelle «société de la surveillance».

[22] Pour mieux comprendre si une activité est couverte ou non par cette «exemption domestique», voir l'Avis 5/2009, sur les réseaux sociaux en ligne (WP 163).

[23] Le problème ne se pose pas dans les organisations (du secteur public ou privé) utilisant des applications informatiques dématérialisées, car la directive s'applique à ces dernières, ainsi qu'à leurs opérations de traitement lorsqu'elles «[sont effectuées] dans le cadre des activités d'un établissement du responsable du traitement» dans l'UE [voir l'article 4, paragraphe 1, point a)]. Le chapitre 5 s'applique donc à ces organisations, que le prestataire de services soit ou non établi dans l'UE.

[24] Cela concerne, par exemple, le consentement des enfants et/ou de leurs parents, les demandes d'accès des autorités policières et judiciaires, les droits d'accès aux comptes internet de personnes décédées par leurs héritiers, et les demandes de tiers.

6. Renforcement de la responsabilité des responsables du traitement des données

72. Au titre de la directive 95/46/CE, le responsable du traitement des données est l'acteur clé qui veille au respect des principes et obligations visant à garantir la protection des données à caractère personnel des personnes physiques. La directive, de manière implicite mais également explicite en de nombreux points, impose au responsable du traitement de respecter les principes de protection des données et de se conformer à certaines obligations spécifiques[25]. Il doit par exemple adresser une notification aux autorités nationales et vérifier préalablement auprès d'elles la légalité des opérations de traitement des données[26]. En outre, le respect des droits des personnes physiques en matière de protection des données implique d'imposer au responsable du traitement les obligations correspondantes, telles que la transmission d'informations[27].

73. Ces obligations s'appliquent aussi, de manière directe ou indirecte, aux sous-traitants si les responsables du traitement des données leur confient tout ou partie des opérations de traitement. Soucieux de préciser les notions de responsable du traitement des données et de sous-traitant des données, le groupe de travail 29 prépare actuellement un avis interprétatif sur la question, qu'il devrait rendre prochainement à la Commission. Cet avis pourrait comprendre de nouvelles recommandations pour un futur cadre juridique.

Intégration de la protection des données dans les organisations

74. Les dispositions pertinentes de la directive 65/46/CE forment une base incontestablement solide pour la protection des données à caractère personnel et devraient être maintenues. Néanmoins, le respect des obligations juridiques existantes est souvent insuffisamment intégré dans les pratiques internes des organisations. Il est fréquent que la protection de la vie privée ne soit pas prise en compte par les technologies et systèmes de traitement de l'information. En outre, la direction, notamment les cadres supérieurs, n'est généralement pas suffisamment au fait des pratiques en matière de traitement des données appliquées dans l'organisation et n'en est donc pas activement responsable. Les scandales liés à la protection des données qui ont éclaté dans certains États membres ces quelques dernières années témoignent de ce constat préoccupant.

75. Tant que la protection des données ne fera pas partie des valeurs et des pratiques communes d'une organisation et que les responsabilités n'en sont pas clairement attribuées, le respect effectif du principe de protection sera compromis et les incidents liés à la protection des données perdureront. Par ailleurs, une telle situation risque de fragiliser la confiance du public dans les entreprises comme dans les administrations publiques. En outre, l'intégration de la protection des données dans les cultures des organisations aidera les autorités chargées de la protection des

---

[25] L'article 6, paragraphe 2, dispose explicitement qu' « [i]l incombe au responsable du traitement d'assurer le respect du paragraphe 1» (qui renvoie aux principes généraux relatifs à la qualité des données).

[26] Voir les articles 18 à 21 de la directive 95/46/CE.

[27] D'autres exemples des droits des personnes concernées comprennent le droit d'accès, de rectification, d'effacement et de blocage, et d'opposition au traitement des données à caractère personnel (articles 10 à 12 et article 14). Ces droits impliquent pour le responsable du traitement l'obligation de les respecter.

données à mener à bien leurs missions de contrôle et de lutte contre la criminalité, comme il est expliqué au chapitre 7, ce qui aura pour effet d'accroître l'efficacité des mesure de protection de la vie privée.

76. Les principes et obligations énoncés dans la directive 95/46/CE devraient être au cœur même de la culture des organisations, à tous les niveaux, au lieu d'être considérés comme un ensemble d'obligations juridiques à valider par le service juridique. Les exigences énoncées par la directive devraient correspondre à des mesures concrètes de protection des données appliquées quotidiennement. Les contrôles en matière de protection de la vie privée devraient être pris en compte dès la conception des technologies et systèmes d'information (voir également le chapitre 4). En outre, au sein des organisations des secteurs public et privé, la responsabilité interne de la protection des données devrait être suffisamment reconnue, renforcée et attribuée de manière spécifique.

77. L'efficacité des dispositions de la directive 95/46/CE repose sur les efforts que déploient les responsables du traitement des données pour atteindre ces objectifs. Elle passe par les mesures proactives suivantes:

- *l'adoption par les responsables du traitement des données de politiques et processus internes* mettant en œuvre les exigences de la directive en ce qui concerne les opérations de traitement spécifiques réalisées par le responsable du traitement. Ces processus et politiques internes devraient être approuvés au plus haut niveau de l'organisation et par conséquent être imposés à l'ensemble du personnel;
- *la mise en place de mécanismes de mise en œuvre des politiques et processus internes, notamment le traitement des plaintes (voir également le chapitre 5),* afin de garantir l'efficacité pratique de ces politiques. Il pourra s'agir notamment de sensibiliser le personnel à la protection des données, de le former et de lui donner des instructions à ce sujet;
- *la rédaction de rapports de conformité et la réalisation d'audits, la certification par des organismes tiers* pour contrôler et évaluer si les mesures internes adoptées pour garantir le respect des obligations permettent de gérer efficacement, de protéger et d'assurer la sécurité des données à caractère personnel (voir également le chapitre 4);
- la conduite d'*études d'impact sur la vie privée*, notamment pour certaines opérations de traitement des données réputées présenter des risques spécifiques pour les droits et libertés des personnes concernées, par exemple en raison de leur nature, de leur portée ou de leur finalité;
- *l'attribution de la responsabilité de la protection des données* à des personnes désignées, directement chargées du respect par leur organisation de la législation sur la protection des données;
- *la certification de la conformité par les cadres supérieurs de l'organisation*, confirmant qu'ils ont mis en place des garanties appropriées pour protéger les données à caractère personnel;
- *la transparence de ces mesures adoptées* vis-à-vis des personnes concernées et du public en général. Les obligations de transparence contribuent à la responsabilisation des personnes en charge du traitement des données (par exemple, publication des politiques de protection de la vie privée sur l'internet, transparence du traitement interne des plaintes et publication dans les rapports annuels).

78. L'article 17, paragraphe 1, de la directive 95/46/CE, impose déjà dans une certaine mesure aux responsables du traitement des données de mettre en œuvre les mesures techniques et d'organisation (le responsable du traitement des données doit «*mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre [...] toute autre forme de traitement illicite*»). Ces mesures peuvent comprendre certaines des recommandations susmentionnées. Toutefois, en pratique, l'article 17, paragraphe 1, n'a pas permis de rendre la protection des données suffisamment efficace dans les organisations en raison, notamment, de la diversité des approches adoptées par les mesures nationales de mise en œuvre.

Principe de responsabilité[28]

79. Pour résoudre ce problème, il conviendrait d'introduire un principe de responsabilité dans le cadre global aux termes duquel les responsables du traitement des données seraient contraints de prendre les mesures nécessaires pour *veiller* au *respect* des obligations et principes essentiels de la directive actuelle lors du traitement des données à caractère personnel. Une telle disposition renforcerait la nécessité de mettre en place des politiques et des mécanismes permettant la mise en œuvre effective des principes et obligations essentiels de la directive actuelle. Elle confirmerait la nécessité de prendre des mesures efficaces donnant lieu à une application interne efficace des obligations et principes essentiels actuellement consacrés dans la directive. En outre, le principe de responsabilité exigerait des responsables du traitement des données qu'ils mettent en place les mécanismes internes nécessaires pour *démontrer leur conformité* aux parties prenantes externes, notamment aux autorités nationales chargées de la protection des données. Au final, la nécessité de prouver que les mesures appropriées ont été prises pour assurer la conformité facilitera considérablement l'exécution des règles applicables.

80. En tout état de cause, les mesures attendues des responsables du traitement des données devraient être modulables et prendre en compte, entre autres critères, le type de la société (sa taille, son statut de société à responsabilité limitée), ainsi que le type, la nature et la quantité de données à caractère personnel qui lui sont confiées.

Autres solutions proactives ou réactives

81. Certaines des mesures décrites précédemment peuvent être considérées comme de bonnes pratiques, qui satisfont par conséquent au principe de responsabilité si elles sont mises en œuvre. La législation pourrait prévoir un système de récompense pour inciter les organisations à appliquer ces mesures.

82. Une autre solution pourrait être plus normative. Par exemple, l'article 17, paragraphe 1, pourrait être rédigé de sorte à proposer d'autres mesures proactives, comme celles évoquées précédemment, que les responsables du traitement des données seraient tenus de mettre en œuvre. Ces mesures devraient viser des objectifs spécifiques et être neutres sur le plan technologique.

83. D'autres mesures seraient de nature plus réactive. Appliquées en cas de traitement illicite des données à caractère personnel, elles pourraient notamment prévoir:

[28] Voir également le point 39 sur la responsabilité.

- *une obligation de notification en cas de violation de la sécurité* des données (voir également les chapitres 2 et 5);
- *le renforcement des compétences des autorités chargées de la protection des données en matière de lutte contre la criminalité*, notamment l'adoption d'obligations concrètes pour garantir une protection efficace des données (voir également le chapitre 7a).

Simplification des notifications

84. Les notifications des opérations de traitement aux autorités nationales chargées de la protection des données pourraient être simplifiées ou réduites. Dans ce contexte, il convient d'examiner le lien entre le respect des exigences susmentionnées et la possibilité de préciser plus avant les obligations administratives, en particulier la notification d'activités de traitement des données aux autorités nationales chargées de la protection des données.

85. La notification contribue à sensibiliser le personnel des organisations aux opérations de traitement de données et aux pratiques liées à leur protection[29]. Elle donne également aux autorités chargées de la protection des données une vision des activités de traitement. Néanmoins, un renforcement des obligations en matière de gouvernance des données et de responsabilité pourrait permettre d'atteindre les mêmes objectifs. Ces mécanismes pourraient contribuer à la mise en œuvre des mesures nécessaires pour respecter les principes et obligations essentiels actuellement consacrés dans la directive et produire les preuves d'un tel respect.

86. Il convient d'examiner si et dans quelle mesure la notification pourrait être limitée aux cas de menace grave contre la protection de la vie privée, ce qui permettrait aux autorités chargées de la protection des données d'être plus sélectives et de concentrer leurs efforts sur ces situations. Même dans de tels cas, la notification pourrait être rationalisée, par exemple, par la communication des résultats des études d'impacts sur la vie privée ou des audits réalisés par des tiers. Elle pourrait être associée à un système d'enregistrement qui imposerait l'inscription de tous les responsables du traitement des données dans un registre tenu par l'autorité chargée de la protection des données, ce qui permettrait d'identifier aisément les organisations en vue d'une application efficace et efficiente de la loi, si nécessaire.

7. Les autorités chargées de la protection des données devraient avoir un rôle plus important et plus précis, et renforcer leur coopération au sein de l'UE

7a. Les autorités chargées de la protection des données

87. À l'heure actuelle, il existe d'importantes disparités entre les 27 États membres en ce qui concerne le rôle des autorités chargées de la protection des données. Ces disparités sont le fruit de l'histoire, de la jurisprudence, de la culture et de l'organisation interne qui varient d'un État membre à l'autre, mais également, à

[29] Ce point de vue est confirmé par le rapport du groupe de travail sur l'obligation de notification aux autorités nationales de contrôle, sur la meilleure utilisation des dérogations et des simplifications et sur le rôle des détachés à la protection des données dans l'Union européenne (WP 106), adopté le 18 janvier 2005.

maints égards, de l'imprécision de la directive 95/46/CE. De plus, cette directive a, dans une certaine mesure, été transposée de manière incomplète dans certains pays, créant d'importantes disparités entre les États membres en ce qui concerne, notamment, le rôle, les ressources et les pouvoirs des autorités chargées de la protection des données.

88. Les nouveaux défis en matière de protection des données (la mondialisation et les évolutions technologiques, voir les chapitres 3 et 4) nécessitent un contrôle ferme, plus homogène et efficace des autorités chargées de la protection des données. Dès lors, le nouveau cadre devrait garantir l'application de normes homogènes en ce qui concerne l'indépendance, les pouvoirs réels et le rôle consultatif de ces autorités dans le processus législatif, mais également leur capacité à définir leur propre programme de travail, notamment en fixant les priorités en matière de traitement des plaintes. De telles normes devraient être adoptées à un haut niveau par des instances qui font autorité.

89. Les autorités chargées de la protection des données doivent être pleinement et réellement indépendantes. L'actuel article 28, paragraphe 1, de la directive 95/46/CE manque de clarté à cet égard, comme le démontre l'affaire C-584/07 (Commission/Allemagne), actuellement examinée par la Cour de justice des Communautés européennes. Dans le nouveau cadre juridique, les autorités chargées de la protection des données devraient bénéficier:

- d'une indépendance institutionnelle totale et ne pas être subordonnées à une quelconque autre autorité gouvernementale;
- d'une indépendance fonctionnelle et ne pas être soumises aux instructions de l'entité contrôlée en ce qui concerne le contenu et l'étendue de ses activités;
- d'une indépendance matérielle. Elles devraient disposer d'une infrastructure adaptée à la conduite ininterrompue de leurs activités, notamment d'un financement suffisant. Les autorités chargées de la protection des données devraient se voir affecter des ressources suffisantes.

90. Les autorités chargées de la protection des données jouent un rôle de plus en plus important dans la lutte contre la criminalité. Elles doivent être en mesure d'agir avec fermeté, audace et stratégie en matière d'intervention et de lutte contre la criminalité. La formulation actuelle de l'article 28 de la directive 95/46/CE a donné lieu à une grande disparité des pouvoirs de lutte contre la criminalité. Le nouveau cadre devrait inviter les États membres à adopter une approche plus homogène, qui dote les autorités chargées de la protection des données des pouvoirs nécessaires, et devrait être plus précis à cet égard que la directive 95/46/CE. Parmi les pouvoirs indispensables, citons la faculté d'infliger des sanctions financières aux responsables du traitement des données et à leurs sous-traitants.

91. Le rôle consultatif des autorités chargées de la protection des données dans le processus législatif est indispensable, car les connaissances acquises par ces autorités lors d'enquêtes et d'actions de contrôle est souvent nécessaire pour améliorer la législation (sur la protection des données). Ce rôle consultatif devrait concerner toutes les mesures et tous les règlements liés à la protection des droits et des libertés des personnes à l'égard du traitement de données à caractère personnel, et pas

uniquement les «mesures réglementaires ou administratives»[30]. L'avis des autorités chargées de la protection des données devrait donc être sollicité avant que le projet de loi ne soit adopté. En outre, le nouveau cadre devrait veiller à ce que ces autorités remplissent un rôle consultatif auprès de leurs parlements nationaux et/ou autres institutions nationales compétentes, lorsque ces derniers participent à la rédaction d'une nouvelle législation de l'UE.

92. Elles devraient être en mesure d'établir leur propre programme de travail, en fixant, notamment, les priorités et les modalités de traitement des plaintes[31]. Elles devraient, en tout état de cause, pouvoir évaluer dans quelle mesure le traitement d'une plainte donnée peut contribuer suffisamment à la protection des données à caractère personnel[32]. Le nouveau cadre devrait permettre aux autorités chargées de la protection des données d'«être sélectives pour être efficaces».

93. Par ailleurs, les autorités chargées de la protection des données doivent assumer la responsabilité de l'usage qu'elles font de leur pouvoir de contrôle accru. Elles devraient être transparentes à cet égard et rendre compte publiquement de leurs modalités d'action et des priorités qu'elles se fixent. La formulation actuelle de l'article 28, paragraphe 5, de la directive 95/46/CE devrait être précisée à cet égard dans le nouveau cadre.

7b. Coopération entre les autorités chargées de la protection des données

Le cadre juridique actuel

94. L'article 29 de la directive 95/46/CE institue le groupe de protection des personnes à l'égard du traitement des données à caractère personnel (groupe de travail 29) en tant qu'organisme institutionnel chargé de la coopération entre les autorités nationales chargées de la protection des données. Le groupe de travail 29 est un organe consultatif et indépendant. Conformément à l'article 30, paragraphe 1, de la directive, il a pour mission de contribuer à la mise en œuvre homogène de la directive, par l'examen de toute question portant sur l'application des dispositions nationales, de donner des avis sur le niveau de protection dans la Communauté et dans les pays tiers, et de conseiller (y compris de sa propre initiative) la Commission sur tout projet de législation communautaire ayant une incidence sur la protection des données ou sur tout autre sujet lié à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté. La Commission est membre du groupe de travail 29 et en assure le secrétariat.

95. Le groupe de travail 29 remplit sa mission dans le cadre de la directive 95/46/CE, comme le prévoit son article 3, paragraphe 2. Dans le domaine de la coopération policière et judiciaire, les autorités européennes chargées de la protection des données ont créé en 2007 le groupe de travail «Police et justice» qui remplit une fonction similaire à celle du groupe de travail 29, mais sans base juridique ni

[30] Article 28, paragraphe 2, de la directive 95/46/CE.

[31] La capacité de choix peut être mise en pratique de différentes manières, par exemple par l'établissement de procédures accélérées pour le traitement des plaintes mineures.

[32] Les critères applicables pour déterminer si une plainte doit être traitée consistent par exemple à vérifier si celle-ci décrit une situation qui concerne un grand nombre de personnes, une violation de la législation sur la protection des données de faible importance et probablement pas un phénomène isolé, et si le traitement de la plainte donnera vraisemblablement lieu à une issue favorable et ne nécessite pas d'efforts disproportionnés.

secrétariat assuré par une institution de l'UE. La décision-cadre 2008/977/JAI, qui introduit les principes de protection des données dans ce domaine, ne prévoit aucune coopération institutionnalisée entre les autorités chargées de la protection des données.

Le fonctionnement du groupe de travail 29

96. Actif depuis plus de 10 ans, le groupe de travail 29 a largement contribué à la réalisation des objectifs de l'article 30 de la directive 95/46/CE. Les résultats d'un grand nombre de ses activités sont présentés sur son site[33].

97. Le groupe de travail 29 cherche constamment à renforcer son efficacité et devrait continuer à prêter une attention particulière à son fonctionnement.
Il devrait notamment s'interroger sur la manière:

- de contribuer efficacement à la mise en œuvre homogène de la législation de l'UE et des lois nationales ainsi qu'à l'application homogène de la législation nationale;
- d'améliorer son efficacité vis-à-vis des institutions de l'UE et en particulier de la Commission, en tenant également compte du rôle hybride de celle-ci en tant que membre, secrétariat et destinataire de la plupart des avis du groupe.

Conséquences pour l'avenir

98. La première priorité consiste à s'assurer que toutes les questions liées au traitement des données à caractère personnel, en particulier dans le domaine de la coopération policière et judiciaire en matière pénale, seront couvertes par les activités du groupe de travail actuel. Un cadre juridique global devrait prévoir un conseiller général et une coopération efficace entre les autorités de contrôle. Pendant une période transitoire, tant qu'aucune modification législative ne sera entrée en vigueur, des modalités appropriées de collaboration étroite devront être trouvées entre le groupe de travail 29 et le groupe de travail «Police et justice».

99. D'autres améliorations ne nécessitent aucune modification législative.

- L'application homogène de la législation nationale transposant la directive 95/46/CE peut être assurée au sein du cadre juridique actuel, par le renforcement des méthodes de travail du groupe et, le cas échéant, par une volonté accrue de ses membres d'inscrire les points de vue du groupe de travail dans la pratique nationale.
- Conformément à l'article 29 de la directive 95/46/CE, le secrétariat du groupe de travail 29 est assuré par la Commission. Le secrétariat devrait travailler en étroite collaboration avec la présidence du groupe de travail 29 et son personnel. Les tâches du secrétariat et de la présidence sont complémentaires. Tous deux devraient travailler en étroite collaboration pour permettre au groupe de travail 29 de mener à bien ses missions aussi efficacement que possible. Le secrétariat gère tous les aspects logistiques des activités du groupe de travail et l'aide à préparer ses avis et documents. La présidence (et la vice-présidence) se consacre essentiellement au processus décisionnel et à la stratégie du groupe de travail 29.

[33] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm

- Les relations entre le groupe de travail et la Commission peuvent encore être améliorées par une description des fonctions essentielles des deux acteurs dans un protocole d'accord. Celui-ci devrait également porter sur les ressources mises à la disposition du groupe de travail 29 pour lui permettre d'exploiter pleinement ses capacités au service de sa mission. Enfin, il devra s'intéresser au fonctionnement du secrétariat, pour veiller à ce que ce dernier et le groupe de travail 29 disposent des ressources suffisantes pour préparer les avis et les documents de travail du groupe. Le groupe de travail 29 lancera une consultation avec la Commission sur l'ensemble de ces points en 2010.

8. Les défis de la protection des données dans le domaine de la police et de la lutte contre la criminalité

100. La protection des données dans le domaine de la police et de la justice est un sujet spécifique qui requiert une attention particulière, compte tenu de la relation complexe entre les activités de l'État visant à garantir la sécurité et la protection des données à caractère personnel des personnes physiques. La spécificité de cette question résulte non seulement de l'ancienne structure en piliers des précédents traités européens, mais est également plus largement reconnue (voir par exemple les exceptions de l'article 13 de la directive 95/46/CE et la déclaration 21 annexée au traité de Lisbonne).

Évolution du contexte communautaire

101. L'entrée en vigueur du traité de Lisbonne offrira de nouvelles perspectives pour le travail législatif dans le domaine de la protection des données. La structure en piliers sera supprimée, et l'article 16 du TFUE crée une base juridique unique pour la protection des données dans presque tous les domaines du droit de l'Union (voir le chapitre 2). Cela ne signifie pas nécessairement que la mise en œuvre des principes de la protection des données en matière policière et judiciaire devrait être identique aux règles applicables aux autres secteurs de la société. La déclaration 21, annexée au traité de Lisbonne, prévoit que des règles spécifiques en matière de lutte contre la criminalité «pourraient s'avérer nécessaires».

102. La protection et l'échange des données seront des thèmes importants du programme de Stockholm. Le processus décisionnel reposera sur la notion de juste équilibre entre les besoins qu'exige la lutte contre la criminalité et ceux liés à la protection des données. De nouvelles mesures ne devraient être adoptées qu'après évaluation adéquate du cadre juridique actuel.

103. La décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale doit être transposée par les États membres avant le 27 novembre 2010. Elle peut être considérée comme un premier pas vers la création d'un cadre général relevant de l'ancien troisième pilier, mais est loin d'être complète. En effet, elle ne s'applique qu'aux situations transfrontalières. Il semble qu'elle ne prévoie pas d'éléments ni d'outils essentiels pour réagir efficacement à l'évolution des méthodes de travail en matière de lutte contre la criminalité.

Changement des priorités dans la lutte contre la criminalité

104. On a assisté ces dernières années à un changement des priorités dans les méthodes de travail des autorités policières et judiciaires, en ce qui concerne l'utilisation des informations (à caractère personnel). Ce changement résulte des besoins croissants d'utilisation de ces informations pour combattre les nouvelles menaces résultant du terrorisme et de la criminalité organisée, mais également des progrès technologiques de ces dernières années.

105. Ce changement des priorités revêt plusieurs aspects:

- l'utilisation d'informations est orientée sur les premières étapes de la chaîne: outre l'utilisation habituelle à des fins d'enquête et de détection d'un crime spécifique, les informations sont recueillies et échangées pour prévenir d'éventuels actes criminels («police préventive »);
- l'utilisation d'informations concerne un groupe plus large de personnes. Des informations sont collectées et échangées, non seulement sur les personnes directement liées à un crime telles que les suspects ou les témoins, mais aussi sur des groupes plus larges de personnes qui ne font pas l'objet d'une enquête (par exemple, les voyageurs, les utilisateurs de services de paiement, etc.);
- les informations utilisées sont de plus en plus associées aux technologies, qui permettent même d'assembler des éléments disparates pour prédire le comportement futur des personnes au moyen d'outils automatisés (extraction de données, profilage);
- les informations utilisées sont de nature différente: elles proviennent non seulement de données obtenues de façon objective (données vérifiées) mais également d'évaluations et d'analyses réalisées dans le cadre d'une enquête (données non vérifiées). Par ailleurs, la distinction entre ces deux types d'informations peut varier selon les États membres;
- l'utilisation accrue, à des fins préventives, d'informations à caractère personnel issues du secteur privé, comme les données bancaires/financières, et les données sur les passagers recueillies par les transporteurs aériens et le SIR;
- les informations collectées dans un but précis et légitime sont de plus en plus exploitées à des fins différentes, parfois incompatibles, et la tendance à leur recoupement est croissante. L'interopérabilité entre les systèmes est un élément important mais n'est pas une question purement technique, compte tenu notamment des risques d'interconnexion des bases de données aux finalités différentes;
- de plus en plus d'autorités participent à l'utilisation de ces données: les autorités policières et judiciaires, au sens strict, mais également d'autres autorités publiques telles que celles chargées du contrôle aux frontières, l'administration fiscale et les services en charge de la sécurité nationale.

106. Ce changement de priorités en matière de lutte contre la criminalité a accru fortement le stockage et l'échange de données à caractère personnel liés aux activités policières et judiciaires. Les possibilités technologiques permettant de combiner aisément les informations peuvent avoir une incidence profonde sur la protection de la vie privée et des données de tous les citoyens et sur leur capacité même de jouir pleinement de leurs droits fondamentaux et de les exercer, notamment dès lors que la liberté de circulation, la liberté de parole et la liberté d'expression sont en jeu.

Défis de la protection des données

107. Dans ce contexte, les défis posés par la protection des données sont immenses. Le futur cadre juridique devrait, en tout état de cause, prendre en compte les facteurs suivants:

- les tendances actuelles peuvent conduire à une surveillance plus ou moins permanente de l'ensemble des citoyens, souvent qualifiée de «société de la surveillance». À titre d'exemple, citons l'utilisation combinée de caméras vidéo intelligentes et d'autres technologies, telles que la reconnaissance automatique des plaques minéralogiques, permettant d'enregistrer les entrées et sorties de tous les véhicules dans une zone donnée;
- les bases de données peuvent servir à l'extraction de données, et des évaluations des risques peuvent être réalisées sur la base du profilage des personnes physiques, ce qui peut conduire à stigmatiser les personnes issues de certains milieux;
- les analyses réalisées sur la base de critères généraux engendrent le risque d'inexactitudes importantes, conduisant à un nombre élevé de faux négatifs et de faux positifs;
- le traitement des données à caractère personnel de personnes non suspectes prend de plus en plus d'ampleur. Des conditions et des garanties spécifiques sont indispensables pour évaluer leur légitimité et leur proportionnalité, et pour éviter toute atteinte aux personnes qui ne sont pas (activement) impliquées dans un délit;
- les données biométriques sont de plus en plus utilisées, notamment l'ADN, ce qui présente des risques spécifiques.

Conditions pour le processus législatif et l'élaboration des politiques

108. Le nombre croissant d'initiatives sectorielles adoptées ou programmées peut facilement conduire au double emploi ou même à des distorsions. Il peut donc s'avérer judicieux de fonder l'échange d'informations sur une stratégie cohérente, à condition que la protection des données soit pleinement prise en compte et intégrée à cette stratégie[34].

109. Il est primordial d'évaluer les instruments juridiques actuels et leur application, en tenant compte des coûts induits par la protection de la vie privée. L'évaluation des mesures actuelles devrait être effectuée avant que de nouvelles mesures ne soient prises. En outre, un examen périodique des mesures existantes devrait être réalisé.

110. La transparence est un élément essentiel. Les personnes concernées devraient disposer d'informations précises sur l'utilisation des informations collectées et sur la logique sous-jacente au traitement. Cette collecte d'informations devrait uniquement être limitée, si nécessaire, à des cas individuels, pour ne pas compromettre les enquêtes et pour une durée limitée. Les droits d'accès et de rectification des personnes concernées devraient être pris en compte dans un contexte transfrontalier pour éviter que ces personnes ne perdent le contrôle de leurs données.

111. Une attention particulière doit être accordée à la transparence et au contrôle démocratique du processus législatif. Une place importante devrait être accordée aux

[34] Une stratégie européenne de gestion des informations, en cours d'élaboration par le Conseil, pourra, si elle est correctement mise en place, s'avérer utile dans ce contexte.

études d'impacts sur la vie privée, à des modes appropriés de consultation des autorités chargées de la protection des données et à un débat parlementaire efficace, aux niveaux national et européen.

112. L'architecture de tout système de stockage et d'échange de données à caractère personnel devrait être bien élaborée. On prendra note des quelques considérations générales suivantes:

- la prise en compte du respect de la vie privée dès la conception et les technologies améliorant la protection de la vie privée (système de certification) devraient déterminer cette architecture; en matière de liberté, de sécurité et de justice, domaines dans lesquels les autorités publiques jouent un rôle prépondérant et où chaque initiative visant à une surveillance accrue des personnes et à un renforcement de la collecte et de l'utilisation des informations à caractère personnel pourrait avoir une incidence directe sur le droit fondamental de ces personnes à la protection de leur vie privée et de leurs données, ces exigences pourraient être rendues obligatoires;
- la limitation des finalités et du nombre de données collectées devrait rester un principe directeur;
- l'accès à d'importantes bases de données doit être configuré de sorte à interdire, de manière générale, la consultation directe en ligne des données stockées, et un système «trouvé/non trouvé» ou dispositif d'indexation est généralement jugé préférable;
- le choix entre des modèles mettant en œuvre un stockage central, à savoir des systèmes dotés d'une base de données centrale au niveau de l'UE et d'un stockage décentralisé, devrait être effectué sur la base de critères transparents et, en tout état de cause, s'accompagner de dispositions strictes prévoyant une définition claire du rôle et des obligations des responsables du traitement, et s'assurer d'un contrôle approprié par les autorités compétentes chargées de la protection des données;
- les données biométriques devraient être utilisées uniquement si le recours à d'autres dispositifs moins intrusifs ne permet pas d'obtenir les mêmes résultats.

113. La dimension extérieure. Il conviendra d'éviter que le système rigoureux d'échange de données à caractère personnel au sein de l'UE soit contourné. Les relations avec les États tiers devraient s'appuyer sur un cadre précis, contraignant pour toutes les parties et reposant sur la notion de niveau de protection adéquat. Le système d'évaluation du caractère adéquat de la protection devrait être apprécié à la suite d'une évaluation par les autorités nationales chargées de la protection des données, si nécessaire réalisée au moyen de mécanismes communs assurant une mise en œuvre cohérente et une grande efficacité.

114. Une attention particulière doit être accordée aux systèmes d'informations à grande échelle dans l'UE et, si nécessaire, des garanties spécifiques pourront être adoptées pour assurer la protection des données.

115. Un contrôle indépendant, de même qu'un contrôle judiciaire et des voies de recours devraient être prévus. En tout état de cause, un contrôle indépendant implique la mobilisation de ressources et de compétences appropriées.

116. La coopération entre les autorités chargées de la protection des données, qui doivent veiller à la licéité du traitement des données, devrait être renforcée à tous égards et être intégrée dans le cadre juridique. Elle devrait également prévoir des mécanismes stables, similaires à ceux actuellement à l'œuvre pour les questions liées au premier pilier, afin de promouvoir une approche harmonisée dans toute l'UE et au-delà.

Pour le groupe de travail «Article 29»	*Pour le groupe de travail «Police et justice»*
Le président	Le président
Alex TÜRK	Francesco PIZZETTI