LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur l'évolution future de l'espace de liberté, de sécurité et de justice

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et en particulier son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et en particulier ses articles 7 et 8,

vu la 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[1],

vu le 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[2], et en particulier son article 41, paragraphe 2,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1. L'objet du présent avis est de contribuer à l'évolution future des politiques de l'Union européenne dans le domaine de la liberté, de la sécurité et de la justice par une intégration plus poussée de la vie privée et de la protection des données dans les activités de toutes les institutions européennes. Il fait suite à deux communications adoptées par la Commission le 11 mars 2014 sur l'avenir de la justice et des affaires intérieures[3], à la résolution adoptée par le Parlement européen le 2 avril 2014 examinant le programme de Stockholm et aux discussions au Conseil européen en vue de la conclusion par le Conseil, pour la première fois, d'orientations stratégiques de la programmation législative et opérationnelle conformément à l'article 68 du TFUE.

2. Il s'agit d'un moment critique pour le rôle de l'Union européenne dans la justice et les affaires intérieures. Nous arrivons à la fin de la période de transition fixée par le traité de Lisbonne, à l'issue de laquelle les pouvoirs de la Commission à engager des recours en manquement et les pouvoirs de la Cour de justice de l'Union européenne deviendront pleinement applicables aux législations européennes relatives à la coopération policière et

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] Voir le point 8 ci-dessous.

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30
Courriel: edps@edps.europa.eu – Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 – Fax: 02-283 19 50

judiciaire en matière pénale[4]. Conformément au traité, la Charte des droits fondamentaux a pris le statut de droit primaire et la Cour de justice, dans de récents arrêts, a clarifié les restrictions à la marge de manœuvre du législateur quand une mesure implique une ingérence dans ces droits[5].

3. En outre, on peut dire que les inquiétudes quant à la vie privée et la protection des données se sont plus intensifiées que jamais au cours des cinq dernières années. En janvier 2012, la Commission a proposé une série de réformes législatives concernant la protection des données dans l'Union européenne[6]. Depuis juin 2013, les révélations sur la surveillance massive des citoyens de l'Union européenne par des agences de renseignement américaines et autres ont fortement porté atteinte à la confiance quant à la confidentialité des informations à caractère personnel. Plus récemment, en avril 2014, dans l'un des deux arrêts susmentionnés, la Cour de justice a annulé la directive relative à la conservation des données[7] au motif de son ingérence excessive dans les droits fondamentaux. L'action au niveau européen en matière de protection des données a véritablement pris une dimension mondiale, ainsi qu'en atteste par exemple le niveau de couverture internationale et de lobbying autour de la réforme du cadre de la protection des données, qui a conduit à près de 4 000 amendements soumis en première lecture au Parlement européen[8].

4. Les défis juridiques, technologiques et sociétaux pour les décideurs politiques et les législateurs en matière de justice et d'affaires intérieures vont certainement s'intensifier au cours de la période qui sera couverte par les lignes directrices stratégiques. En outre, les nouvelles lignes directrices du Conseil européen offrent l'opportunité de proclamer une intention de restaurer la confiance dans la capacité de l'Union européenne à protéger efficacement les individus. Pour cette raison, nous suggérons au Conseil européen d'aborder explicitement les thèmes suivants dans les nouvelles lignes directrices:

    a. les volumes considérables de données à caractère personnel dont le traitement est requis par de nombreuses législations et politiques européennes en matière de liberté, de sécurité et de justice;

    b. la fragilité de toute mesure qui ne respecte pas les droits fondamentaux, comme nous l'avons vu avec la directive relative à la conservation des données, mais qui

[4] Les dispositions transitoires cessent de s'appliquer le 1er décembre 2014; article10, protocole 36 sur les dispositions transitoires, annexé au traité de Lisbonne.

[5] Voir, dans ce contexte, les arrêts du 9 novembre 2010, Volker und Markus Schecke et Eifert (C-92/09 et C-93/09), et en particulier du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a. (C-293/12 et C-594/12). Dans le premier arrêt, la Cour de justice avait souligné la nécessité pour le législateur d'envisager d'autres solutions suffisamment moins intrusives pour une mesure particulière.

[6] COM(2012) 11 final; COM(2012) 10 final.

[7] Directive 2006/24/CE, JO L 105/54.

[8] À l'issue de la première lecture, le Parlement européen a adopté la résolution législative concernant une proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)] (procédure législative ordinaire: première lecture).

vaut aussi pour d'autres initiatives en cours, telles que le paquet de mesures «Frontières intelligentes»[9] et les divers instruments liés aux dossiers passagers[10];

c. l'importance d'adopter dès que possible un cadre solide et modernisé de protection des données au sein de l'Union européenne, qui devrait aussi servir de référence pour les politiques extérieures européennes; et

d. la nécessité d'intégrer les questions de vie privée et de protection des données dans le développement de toutes nouvelles politiques et législations en matière de liberté, de sécurité et de justice.

5. Ayant participé à un exercice similaire il y a cinq ans, nous proposons, dans le présent avis, de travailler avec les institutions européennes à l'amélioration de la qualité de la législation du point de vue de la protection des données, dans le cadre d'un nouveau modèle de coopération[11].

2. PERSPECTIVES INSTITUTIONNELLES SUR L'AVENIR DE L'ESPACE DE LIBERTÉ, DE SÉCURITÉ ET DE JUSTICE

6. «Le programme de Stockholm – une Europe ouverte et sûre qui sert et protège les citoyens» (ci-après le «programme de Stockholm»)[12], adopté conformément aux conclusions du Conseil européen les 10 et 11 décembre 2009, a été la troisième déclaration d'intention successive pluriannuelle en matière de justice et d'affaires internes[13]. Il a été rendu public en juin 2009 par une communication de la Commission intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens». L'avis du CEPD publié le 13 juillet 2009 a reconnu l'accent mis par la Commission sur la protection des droits fondamentaux, et en particulier sur la protection des données à caractère personnel, dans le contexte de l'action européenne en matière de citoyenneté, de justice, de sécurité, d'asile et d'immigration. En particulier, nous nous sommes réjouis de l'appel à un régime complet de protection des données couvrant tous les domaines relevant de la compétence de l'Union et de la réaffirmation de principes de base, tels que celui de la limitation des finalités. La Commission a envisagé le développement d'un «modèle européen en matière d'échange d'informations» et d'une «stratégie européenne de gestion de l'information», qui, nous l'espérons, refléterait correctement ces principes et bonnes pratiques.

7. Les 19 et 20 décembre 2013, le Conseil européen, conformément aux fonctions que lui confère l'article 68 du TFUE, a annoncé son intention (pour la première fois en vertu des

[9] Voir l'avis du CEPD du 18 juillet 2013 sur les propositions de règlement établissant un système d'entrée/sortie (EES) et de règlement établissant un programme d'enregistrement des voyageurs (RTP).
[10] Ceci comprend un système européen pour les dossiers passagers [COM(2011) 32 final] et une proposition éventuelle sur le transfert de données de passagers à des pays tiers (http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_home_004_transfer_pnr_data_3rd_countries_en.pdf [consulté le 3 juin 2014]).
[11] Voir, sur cette approche, de façon plus générale, le document stratégique 2014 du CEPD, «The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience», publié sur le site web du CEPD.
[12] JO C 115 du 4 mai 2010, p. 1.
[13] COM(2009) 262 final.

traités actuellement en vigueur) de définir des «orientations stratégiques de la future programmation législative et opérationnelle dans l'espace de liberté, de sécurité et de justice ('post-Stockholm')»[14].

8. Le 11 mars 2014, deux communications de la Commission au Parlement européen et au Conseil, au Comité économique et social européen et au Comité des régions, ont été adoptées autour de ces questions: la première communication, à savoir «L'agenda de l'UE en matière de justice pour 2020 – Améliorer la confiance, la mobilité et la croissance au sein de l'Union»[15], était organisée selon les concepts de «consolidation» de mesures existantes par l'intermédiaire, notamment, d'une formation plus judiciaire, de la «codification» des législations civiles et commerciales, des droits des consommateurs et des législations pénales, et par l'identification de mesures visant à «compléter» la confiance mutuelle, la croissance économique et les droits des citoyens. La deuxième communication, à savoir «Faire de l'Europe ouverte et sûre une réalité»[16], contenait des suggestions plus spécifiques sur la migration légale, telles que des évaluations de coordination sur la migration professionnelle, la migration irrégulière, la modification du code européen des visas, l'asile (notamment une reconnaissance mutuelle des décisions) et la sécurité, telles que de nouvelles législations sur le contrôle des armes à feu et des traités internationaux sur les dossiers passagers. Il semblerait que la Commission, contrairement au Parlement et au Conseil, ne juge plus intéressante une vision unique et cohérente sur l'avenir de l'espace de liberté, de sécurité et de justice.

9. Le 2 avril 2014, le Parlement européen a adopté une résolution sur le programme de Stockholm[17]. La résolution demandait au Conseil européen de mettre en œuvre un «*habeas corpus* numérique européen» sur les droits fondamentaux afin d'accélérer l'adhésion à la Convention européenne des droits de l'homme, afin que le Parlement joue un rôle central dans l'évaluation et la définition de politiques de sécurité intérieure dans le cadre d'une nouvelle Stratégie de sécurité intérieure à partir de 2014 et pour une «vision destinée à préparer l'avenir en ce qui concerne la façon de concevoir et d'optimiser l'échange de données à des fins policières au sein de l'UE tout en garantissant les droits fondamentaux, notamment un solide niveau de protection des données». Plus généralement, le Parlement demandait une «coopération plus étroite et un meilleur échange d'informations entre les institutions et les agences européennes, d'une part, et les États membres, d'autre part, [afin] d'améliorer la conception et la mise en œuvre de la politique» et soutenait que «l'amélioration de la qualité de la législation de l'Union [...] exige un effort conjoint de la part des États membres et des institutions européennes».

10. Parallèlement, le Conseil a mené une série de discussions sur l'avenir de la justice et des affaires intérieures, qui sera aussi abordé lors des délibérations du Parlement européen nouvellement élu. Tout comme la Commission, le Conseil a eu tendance à aller vers des

[14] EUCO 217/13. Tandis que les précédents programmes pluriannuels s'appliquaient pour des périodes de cinq ans, coïncidant largement avec les mandats des collèges de commissaires et parlementaires, le calendrier de l'ensemble des orientations stratégiques envisagées reste obscur. Le Conseil a évoqué la possibilité d'aligner les nouvelles orientations sur le cadre financier pluriannuel actuel de sept ans, 2014-2020.
[15] COM(2014) 144 final.
[16] COM(2014) 154 final.
[17] Résolution du Parlement européen du 2 avril 2014 sur l'examen à mi-parcours du programme de Stockholm, [2013/2024(INI)].

priorités politiques larges, plutôt que vers une programmation détaillée des 10 dernières années, une consolidation et une simplification des mesures existantes plutôt qu'une nouvelle législation et des approches fondées sur des données probantes sur la base d'analyses d'impact.

3. LA PROTECTION DES DONNÉES ET LE PROGRAMME DE STOCKHOLM

L'urgence d'un cadre complet et solide persiste

11. Depuis l'adoption du programme de Stockholm, l'Union a entrepris des démarches considérables pour renforcer les droits fondamentaux, en particulier les droits à la vie privée et à la protection des données. La Charte a acquis force obligatoire avec l'entrée en vigueur du traité de Lisbonne, et l'article 16 du TFUE impose à l'Union de définir des règles en matière de protection des données applicables à toutes les activités relevant du droit communautaire. L'adoption d'un nouveau cadre juridique exhaustif pour la protection des données est particulièrement critique. Les étapes clés de la protection des données pendant la période de mise en œuvre du programme de Stockholm ont été les propositions de la Commission de janvier 2012 pour la réforme du cadre de protection des données et la résolution législative de mars 2014 sur la réforme par le Parlement européen. Il est regrettable que les avancées aient été moins rapides au Conseil, et le CEPD continue à inciter toutes les parties à trouver un accord dès que possible.

12. La proposition ambitieuse de remplacer l'acte législatif central existant sur la protection des données, la directive 95/46/CE, par un règlement directement applicable (ci-après le «règlement général sur la protection des données») promet de renforcer les droits individuels, d'accroître la responsabilisation des responsables du traitement des données, de renforcer la supervision nationale de la conformité et d'apporter une plus grande certitude juridique aux entreprises.

13. La directive 95/46/CE ne s'applique pas aux activités de l'État dans le domaine du droit pénal (article 3, paragraphe 2) et elle donne aux États membres la possibilité de restreindre les droits et obligations si cela est nécessaire pour préserver, entre autres, «la prévention, la recherche, la détection et la poursuite d'infractions pénales» (article 13, paragraphe 1). Le traitement de données dans le cadre de la coopération policière et judiciaire en matière pénale peut avoir un impact particulièrement fort sur la vie des personnes. L'instrument actuel (la décision-cadre 2008/977/JAI du Conseil) ne couvre cependant que le traitement de données au niveau transfrontalier et accorde un vaste pouvoir discrétionnaire aux États membres sur la façon dont les principes sont appliqués. La directive proposée pour remplacer la décision-cadre 2008/977/JAI s'appliquerait au traitement national, sans toutefois modifier ni améliorer les diverses règles existantes figurant dans les instruments de coopération policière et judiciaire.

14. Par conséquent, le CEPD a regretté que la Commission laisse passer une occasion unique de proposer un cadre complet unique offrant un niveau de protection élevé[18]. Si le législateur insiste sur un instrument distinct pour la coopération policière et judiciaire, la proposition de directive doit offrir un niveau de protection équivalent à celui de la proposition de règlement. Les écarts évidents entre les deux instruments, tels que le

[18] Avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012.

manque de clarté quant aux responsabilités lorsqu'il existe un ensemble d'acteurs et de finalités en matière de traitement de données, doivent être traités.

Premiers efforts à évaluer

15. Dans le domaine des affaires intérieures, la Commission a présenté en décembre 2012 un «modèle européen en matière d'échange d'informations», correspondant à la stratégie de gestion de l'information prévue par le programme de Stockholm[19]. Ce document, dont la conclusion était que ni les nouvelles bases de données dans le droit communautaire, ni les nouveaux instruments européens en matière d'échange d'informations n'étaient nécessaires, constituait une première étape bienvenue dans l'évaluation de l'efficacité de l'utilisation de données dans la lutte contre la criminalité, que le CEPD réclamait depuis longtemps.

16. Dans l'ensemble, toutefois, les normes de protection des données dans les activités de justice et d'affaires intérieures restent un patchwork qui, selon les termes du Parlement européen, est «complexe et fragmenté et qui conduit à une utilisation inefficace des instruments disponibles ainsi qu'à une responsabilisation et à un contrôle démocratique inadéquats à l'échelle de l'Union»[20].

Mesures spécifiques

17. La nécessité de conditions strictes et spécifiques concernant la divulgation de données à caractère personnel par des particuliers à des autorités répressives a été clairement soulignée par la Cour de justice dans un arrêt portant sur la directive relative à la conservation des données[21]. Toutefois, comme illustré notamment par l'accord passé avec les États-Unis sur le programme de surveillance du financement du terrorisme, il existe une tendance qui consiste à accorder aux autorités répressives un accès aux données à caractère personnel détenues par le secteur privé. C'est l'une des principales raisons pour lesquelles le Parlement européen a rejeté le premier accord avec les États-Unis[22]. En outre, il existe une tendance plus générale (voir, par exemple le règlement Eurodac, les propositions pour les dossiers passagers et le paquet de mesures «Frontières intelligentes») qui consiste à accorder aux autorités répressives un accès aux données à caractère personnel d'individus, qui ont été collectées à d'autres fins[23].

18. Nous avons régulièrement fait part de nos inquiétudes concernant ces propositions. La résistance à toute initiative en la matière reflète la grande sensibilité du public à l'égard de mesures qui peuvent interférer avec ses droits fondamentaux (le rejet par le Parlement européen de l'*Anti-Counterfeiting Trade Agreement* (ACTA, accord commercial international anti-contrefaçon) est un cas majeur analogue en dehors de l'espace de liberté, de sécurité et de justice), qui est devenue encore plus marquante après les

[19] COM(2012) 735 final.
[20] Point 66, résolution 2013/2024(INI).
[21] Voir la note de bas de page 5 ci-dessus.
[22] Voir le document de travail des services de la Commission, SEC(2011) 438 final.
[23] Voir, par exemple, l'avis du CEPD du 15 décembre 2010 sur la création du système «Eurodac» pour la comparaison des empreintes digitales, Eurodac, et avis du 18 juillet 2013 sur les propositions de règlement établissant un système d'entrée/sortie (EES) et de règlement établissant un programme d'enregistrement des voyageurs (RTP).

révélations de l'Agence nationale de la sécurité (NSA) en 2013. En outre, des parlementaires ont critiqué à maintes reprises la directive relative à la conservation des données avant son annulation par la Cour de justice. Les législations nationales relatives à la conservation des données sont désormais susceptibles d'être contestées sur le fondement d'un manque de proportionnalité et de garanties suffisantes, comme mis en évidence par la Cour de justice.

4. L'ESPACE DE LIBERTÉ, DE SÉCURITÉ ET DE JUSTICE ET LA PROTECTION DES DONNÉES: RISQUES ET OPPORTUNITÉS

Évaluation stratégique de la nécessité de collecter et traiter des données à caractère personnel

19. Les révélations de l'année passée concernant les programmes de surveillance massive ont évoqué de la façon la plus dramatique et concrète possible l'urgence à traiter les intérêts des individus, pas uniquement en tant que consommateurs de services en ligne, mais en tant que citoyens jouissant des droits fondamentaux à la vie privée et à la protection des données à caractère personnel. Un cadre de protection des données harmonisé et pertinent reflète à la fois les valeurs fondamentales et la mission économique de l'Union et, comme une politique judiciaire globale, devrait être considéré comme «un soutien au redressement économique, à la croissance et aux réformes structurelles»[24]. La protection des données peut jouer un rôle clé dans la démonstration de la valeur ajoutée d'une approche européenne au sein de l'espace de liberté, de sécurité et de justice.

20. Le CEPD a demandé à la Commission d'apprécier l'ingérence dans les droits fondamentaux à la lumière des évolutions technologiques, des développements liés aux systèmes informatiques à grande échelle et de l'utilisation croissante de données initialement collectées à des fins sans rapport avec la lutte contre la criminalité, ainsi que l'efficacité pour la sécurité publique de la tendance actuelle à un contrôle élargi, systématique et proactif de personnes non suspectées et de sa réelle utilité dans la lutte contre la criminalité[25].

21. Un certain nombre de mesures et propositions de mesures, qui envisagent le traitement de données à caractère personnel, n'ont pas abouti car elles ne respectaient pas suffisamment les droits à la vie privée et à la protection des données ce qui, selon nous, est dû à l'absence d'évaluation stratégique et systématique des besoins et objectifs politiques futurs. Une telle évaluation devrait être faite par l'intégration des questions de protection des données dans des analyses d'impact d'ordre général, de la question de savoir si les objectifs pourraient être atteints par une meilleure mise en œuvre des mesures existantes ou par d'autres moyens moins intrusifs[26], et par le renforcement de la qualité des données, ainsi que des droits et voies de recours des personnes concernées.

[24] COM(2014) 144 final, p. 3.
[25] Avis du CEPD sur la Communication de la Commission au Parlement européen et au Conseil intitulée «Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen d'échange d'informations (EIXM)» du 29 avril 2013.
[26] Selon l'arrêt Volker und Markus Schecke et Eifert, précité, points 81 et 86.

22. La Commission a l'intention de revoir et mettre à jour la stratégie de gestion intégrée des frontières avec la possibilité de systèmes et plateformes «intégrés». Elle envisage en outre un examen conjoint du Parlement, de la Commission et des États membres de la Stratégie de sécurité intérieure[27]. Le Conseil, quant à lui, a évoqué la nécessité d'étudier une «interconnexion poussée des systèmes d'information, de communication et de données» dans le domaine de la sécurité intérieure. Ces exercices permettront d'évaluer les politiques dans le domaine des affaires intérieures, y compris des initiatives telles que «Frontières intelligentes» qui font l'objet de discussions depuis des années. L'impact sur la protection des données doit faire partie intégrante de cette évaluation. Dans ce cadre, et compte tenu de l'appel du Parlement européen à un *habeas corpus* numérique européen, l'Union devrait rassembler des avis sur la surveillance massive[28], plus particulièrement en ce qui concerne les arrêts pertinents de la Cour de justice.

Comprendre le réel impact de mesures spécifiques sur les citoyens

23. La Commission reconnaît qu'il est nécessaire de continuer à centrer sur les citoyens l'approche de l'espace de liberté, de sécurité et de justice. Dans ses communications sur l'avenir de la justice et des affaires intérieures, la Commission illustre la position de plusieurs États membres, à savoir que l'Union devrait consolider les progrès réalisés, contrôler et évaluer les mesures existantes, plutôt que chercher à adopter une législation plus vaste pour le principe[29]. Une approche centrée sur les citoyens qui aborde les intérêts et les droits fondamentaux des citoyens semblerait tout à fait judicieuse, en particulier compte tenu des défis politiques et juridiques épineux pour la politique de l'Union. Une partie des objectifs politiques généraux devrait toujours consister à réduire l'ingérence dans le droit à la vie privée et mieux garantir la protection des données à caractère personnel.

24. Toutefois, comme démontré par le rapport sur les voies de recours judiciaires récemment publié par l'Agence des droits fondamentaux, le citoyen ordinaire pâtit du manque d'information et des coûts prohibitifs liés à l'obtention d'une réparation pour un traitement de données illégal[30]. Bien que la Commission relève qu'une «coopération étroite entre les autorités nationales ou les organes administratifs est particulièrement importante pour l'efficacité de certains droits européens»[31], les nouvelles lignes directrices stratégiques doivent ériger en priorité l'identification d'étapes pratiques permettant aux individus de faire respecter la protection de leurs données à caractère personnel. Ceci serait conforme à la demande de la Commission concernant des «initiatives complémentaires» qui «faciliteront les vies des citoyens».

25. Des analyses d'impact et une évaluation fondée sur des données probantes devraient aborder le réel effet de mesures qui impliquent le traitement de données à caractère personnel, en termes de nombre de personnes affectées, de risques et de garanties contre

[27] COM(2014) 154 final, p. 9.
[28] Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures [2013/2188(INI)], points 131, 132 et 133.
[29] COM(2014) 144 final, p. 5 à 8, et COM(2014) 154 final, p. 13.
[30] Agence des droits fondamentaux, «Access to data protection remedies in EU Member States», 2013.
[31] COM(2014) 144 final, p. 6.

toute utilisation abusive de ces données, ainsi que les voies de recours ouvertes aux personnes concernées en cas d'abus. La mise en œuvre de mesures et d'activités opérationnelles dépendant fortement du traitement de données à caractère personnel, y compris celles intervenant dans le cadre du cycle politique européen sur la criminalité grave et organisée, devrait aussi tenir compte de toutes les situations ou toutes les allégations d'abus ainsi que des besoins de formation traités[32]. En l'espèce, une considération d'ordre général est l'indépendance des autorités nationales de contrôle, dont l'importance a été renforcée par la Cour de justice dans plusieurs arrêts récents[33], et la façon dont le contrôle peut être coordonné conformément à la pratique actuelle avec Eurodac, les douanes, VIS et SIS II.

Codification et normalisation: une occasion de rapiécer le patchwork

26. Dans le domaine de la justice, la Commission est favorable à la codification des législations, pratiques et jurisprudences existantes dans les domaines du droit civil et commercial, des droits des consommateurs et du droit pénal, convaincue que cela simplifierait, sensibiliserait et améliorerait la confiance mutuelle et supprimerait les incohérences et les règles contradictoires en matière de liberté, de sécurité et de justice[34]. Quant à savoir ce qu'une telle codification pourrait impliquer, la réponse est difficile. Le CEPD a plaidé à maintes reprises pour une norme plus cohérente concernant la protection des données en la matière, plutôt que la panoplie actuelle de normes qui milite contre une certitude juridique pour toutes les parties concernées, qu'il s'agisse d'autorités compétentes, de l'industrie ou des citoyens. Un exercice de codification devrait être étendu à tous les instruments dans le domaine de la liberté, de la sécurité et de la justice, qui ont un impact sur le droit à la protection des données à caractère personnel, tout en apportant suffisamment de flexibilité pour satisfaire aux intérêts publics légitimes.

27. Dans le domaine des affaires intérieures, la Commission renvoie au rôle du système d'information de Schengen dans la garantie de la sécurité et de la liberté de mouvement, ainsi qu'à la nécessité de revoir le code des visas de Schengen et de compléter «le déploiement dans le monde entier du système d'information sur les visas». La Commission envisage une évaluation de l'impact d'un système «basé plus sur l'appréciation des individus que [sic] sur les nationalités»[35]. Une approche mieux calibrée du traitement des données à caractère personnel, telle que celle mise en place dans le cadre du VIS et du SIS II, est judicieuse. L'un des griefs formulés par la Cour de justice contre la directive 2006/24/CE était qu'elle ne nécessitait pas de lien entre les données et une menace pour la sécurité publique et ne se limitait pas à des individus, périodes et lieux spécifiques dès lors que le traitement des données était susceptible d'aider à la prévention, la recherche ou la poursuite d'infractions graves[36].

[32] COM(2014) 154 final, p. 9.
[33] Arrêts du 9 mars 2010, Commission / Allemagne (C-518/07); du 16 octobre 2012, Commission / Autriche (C-614/10) et du 8 avril 2014, Commission / Hongrie (C-288/12).
[34] COM(2014) 144 final, p. 8 et 9.
[35] COM(2014) 154 final, p. 6.
[36] *Digital Rights Ireland*, point 59.

28. Un pas vers une évaluation des risques individuels impliquerait vraisemblablement la collecte et l'analyse d'informations sur certains individus provenant de multiples sources. Tout comme il serait implicitement nécessaire de mettre en place des mécanismes de contrôle de la qualité des données, il serait nécessaire d'accorder une attention particulière, dans le cadre de l'évaluation envisagée d'une telle approche, à l'appréciation de l'ingérence dans les droits à la vie privée et à la protection des données à caractère personnel des individus[37]. Il sera essentiel de garantir des règles claires et précises pour un tel changement politique, définissant les responsabilités des responsables du traitement, en particulier s'il existe une possibilité de sous-traiter la collecte d'informations sur les visas.

Coopération dans le secteur privé

29. Dans sa communication, la Commission met clairement l'accent sur le rôle du secteur privé dans la mise en œuvre d'objectifs d'affaires internes. Ceci inclut de multiples mesures, y compris la proposition de cadre européen pour le traitement de données de dossiers passagers, la méthode de traitement de l'accès aux données de télécommunication et de leur utilisation suite à l'annulation de la directive 2006/24/CE, l'«intensification» de la coopération sur la cybercriminalité par le Centre européen de lutte contre la cybercriminalité, la proposition du nouveau paquet de mesures contre le blanchiment d'argent, et la coopération entre Europol et le secteur privé dans le cadre d'un nouveau règlement Europol.

30. L'accès par les autorités répressives à des données à caractère personnel qui ont été collectées à d'autres fins a soulevé de grandes inquiétudes. Il s'agit d'une exception au principe de limitation des finalités et, par conséquent, un tel accès doit respecter les critères stricts énoncés par la législation relative à la protection des données et les articles 7 et 8 de la Charte. Ceci requiert que des objectifs politiques soient clairement définis et qu'une précision procédurale et des garanties suffisantes contre les abus soient prévues. Pour les citoyens, le danger d'une coopération accrue entre le secteur public et privé en matière répressive, combiné à un double cadre, est une diminution de la responsabilisation et de la transparence. Ceci est encore plus évident si la coopération se fait de façon volontaire. L'identité du responsable du traitement chargé de garantir la conformité doit être claire, tout comme les règles de protection des données applicables. Il doit exister une base légale plus explicite pour une telle coopération, et une finalité légitime et clairement définie pour le traitement des données.

Coopération de pays tiers

31. La Commission et le Conseil attachent tous deux beaucoup d'importance à l'interaction avec des pays tiers, notamment concernant la cybercriminalité et le trafic d'êtres humains. La Commission a l'intention d'évaluer l'efficacité des accords existants avec des pays tiers concernant l'échange d'informations à des fins répressives[38]. Parallèlement, elle

[37] Sur les risques du développement de profils sur la base de critères d'évaluation inconnus et évolutifs, voir l'avis du CEPD du 25 mars 2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.
[38] COM(2014) 154 final, p. 10.

continue à travailler en vue d'un accord-cadre Union européenne / États-Unis sur la protection de la vie privée et des données et sur les mécanismes de réparation pour les citoyens européens, tout en examinant l'accord conclu avec le Canada au sujet des dossiers passagers[39].

32. Le CEPD soutient l'objectif de conclusion d'accords établissant des cadres juridiques clairs pour ces échanges de données entre les autorités répressives, car ils sont nécessaires et apportent de meilleures garanties pour la protection des données. Cependant, toute obligation imposée par un accord international ne saurait nuire au principe selon lequel des mesures européennes doivent respecter les droits fondamentaux, qui ne peuvent être violés par des activités de surveillance excessive[40]. Un accord ne peut légitimer des transferts de données massifs dans un domaine (le domaine répressif) dans lequel l'impact sur les individus est particulièrement grave et dans lequel des garanties strictes et fiables sont, dès lors, d'autant plus nécessaires, en particulier pour éviter tout traitement ultérieur à des fins incompatibles, définir des conditions claires pour des transferts à d'autres autorités ou pays tiers et garantir des droits applicables, y compris des mécanismes de réparation judiciaire pour des personnes concernées dans l'Union européenne. Lorsque l'exception de sécurité nationale est invoquée, les exceptions doivent être définies avec précision et avec des garanties et limitations appropriées.

Recommandations sur la façon d'intégrer les questions de vie privée et de protection des données

33. Selon nous, il est essentiel que les questions de vie privée et de protection des données soient totalement intégrées dans l'élaboration de toute nouvelle politique et législation en matière de liberté, de sécurité et de justice. Dans ce contexte, les actions pourraient être les suivantes:

    - intégrer les questions de protection des données dans des analyses d'impact générales;
    - évaluer d'autres moyens moins intrusifs pour atteindre des objectifs politiques[41];
    - renforcer la qualité des données ainsi que les droits et voies de recours des personnes concernées;
    - évaluer l'échange d'informations par rapport aux objectifs politiques;
    - garantir que les accords internationaux conclus avec des pays tiers respectent le droit des citoyens européens à la protection des données.

[39] Voir l'avis du CEPD sur les propositions de décisions du Conseil relatives à la conclusion et la signature de l'accord entre le Canada et l'Union européenne sur le traitement et le transfert de données des dossiers passagers, 30 septembre 2013.
[40] Voir l'arrêt du 3 septembre 2008, Kadi et Al Barakaat International Foundation / Conseil et Commission (C-402/05 P et C-415/05 P); voir également la résolution 2013/2188(INI) du Parlement européen, point 312.
[41] Selon l'arrêt Volker und Markus Schecke et Eifert, précité, points 81 et 86.

5. VERS UN NOUVEAU MODÈLE DE COOPÉRATION

34. Dans les années à venir, les institutions européennes auront besoin d'une gamme d'outils d'élaboration des politiques plus sophistiquée, garantissant que toute mesure en matière de liberté, de sécurité et de justice empiétant sur les droits à la vie privée et à la protection des données soit proportionnée à ses objectifs, précise dans ses termes et exhaustive dans ses garanties contre les abus. Nous recommandons que les références à ces outils soient mentionnées dans les lignes directrices stratégiques du Conseil européen. Dans notre document stratégique «The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience»[42], nous avons annoncé notre intention de développer une «boîte à outils politiques», et notamment des conseils généraux pour le législateur sous la forme de directives thématiques ou sectorielles, par exemple. La boîte à outils serait destinée à aider les institutions à prendre des décisions en toute connaissance de cause sur les impacts de nouvelles propositions sur la protection des données et pourrait être particulièrement utile dans l'espace de liberté, de sécurité et de justice.

35. Nous sommes disposés à travailler avec les institutions pour élaborer une stratégie et une méthodologie pratique garantissant la protection des données afin de permettre à l'Union d'atteindre des objectifs légitimes de façon plus efficace et efficiente[43]. Des recommandations spécifiques à un secteur pourraient dessiner les étapes pratiques de l'évaluation de la légitimité des finalités, ainsi que de la proportionnalité et de l'identification de normes minimales. L'objet de ces lignes directrices serait d'apporter suffisamment de garanties aux individus dont les données sont traitées, afin de les protéger contre le risque d'utilisation abusive et contre le risque d'accès et d'utilisation illicites[44]. Les lignes directrices devraient également contribuer à la qualité du processus législatif à tous les niveaux, dès lors qu'une ingérence proportionnée dans les droits fondamentaux peut être justifiée par des intérêts publics légitimes. Cet effort tiendra compte de l'évolution de la jurisprudence énonçant des critères d'évaluation de la nécessité et de la proportionnalité d'une mesure et, évidemment, des progrès suffisants en vue de l'adoption du cadre révisé de la protection des données.

6. CONCLUSIONS ET RECOMMANDATIONS

36. La valeur ajoutée de l'action de l'Union en matière de liberté, de sécurité et de justice est fréquemment remise en question, en particulier par les États membres. L'avantage tient à la garantie d'une approche cohérente, par exemple par la conception de systèmes interopérables proportionnés qui peuvent aussi être bénéfiques pour la sécurité et la protection des données. Selon nous, les nouvelles lignes directrices stratégiques sont une excellente opportunité pour les institutions de donner suite aux leçons tirées et de développer une boîte à outils destinée à remédier aux garanties souvent insuffisantes concernant le droit fondamental à la protection des données à caractère personnel.

[42] Voir la note 11.
[43] Le document stratégique du CEPD propose d'accepter des protocoles d'accord avec chaque institution afin de les aider à améliorer la qualité de la législation.
[44] *Digital Rights Ireland*, points 54, 60, 62, 65 et 67.

37. L'Union doit montrer qu'elle a tiré les leçons des cinq dernières années, c'est-à-dire qu'elle ne peut adopter de mesures qui, à y regarder de plus près, interfèrent avec les droits fondamentaux et ne remplissent pas les critères de nécessité et de proportionnalité. Comme la Commission l'a répété à maintes reprises, la Charte doit désormais servir de référence pour les politiques et législations européennes. Le CEPD se tient prêt à apporter son assistance dans ce processus.

38. Les nouvelles lignes directrices du Conseil européen sont une bonne occasion pour l'Union de montrer son intention de restaurer la confiance en sa capacité à protéger efficacement les individus. Pour cette raison, nous suggérons que le Conseil européen aborde explicitement les thèmes suivants dans les nouvelles lignes directrices:

    a. les volumes considérables de données à caractère personnel dont le traitement est requis par de nombreuses législations et politiques européennes en matière de liberté, de sécurité et de justice;

    b. la fragilité de toute mesure qui ne respecte pas les droits fondamentaux, comme nous l'avons vu avec la directive relative à la conservation des données, mais qui vaut aussi pour d'autres initiatives en cours, telles que le paquet de mesures «Frontières intelligentes» et les divers instruments liés aux dossiers passagers;

    c. l'importance d'adopter dès que possible un cadre solide et modernisé de protection des données au sein de l'Union européenne, qui devrait aussi servir de référence pour les politiques extérieures européennes; et

    d. la nécessité d'intégrer les questions de vie privée et de protection des données dans le développement de toutes nouvelles politiques et législations en matière de liberté, de sécurité et de justice.

39. Des actions garantissant que les questions de vie privée et de protection des données sont totalement intégrées dans le développement de toute nouvelle politique et législation en matière de liberté, de sécurité et de justice pourraient être les suivantes:

    - intégrer les questions de protection des données dans des analyses d'impact générales;
    - évaluer d'autres moyens moins intrusifs pour atteindre des objectifs politiques;
    - renforcer la qualité des données, ainsi que les droits et voies de recours des personnes concernées;
    - évaluer l'échange d'informations par rapport aux objectifs politiques; et
    - garantir que les accords internationaux conclus avec des pays tiers respectent le droit des citoyens européens à la protection des données.

Fait à Bruxelles, le 4 juin 2014

(signé)

Peter HUSTINX