COMMISSION EUROPÉENNE

Bruxelles, le 2.2.2011
SEC(2011) 133 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant la

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

relative à une approche commune de l'utilisation des données des dossiers passagers

{COM(2011) 32 final}
{SEC(2011) 132 final}

1. PROCÉDURE ET CONSULTATION DES PARTIES INTÉRESSÉES

Le 6 novembre 2007, la Commission a adopté une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* - PNR) à des fins répressives[1]. La proposition était accompagnée d'une analyse d'impact[2]. Cette proposition a fait l'objet de discussions approfondies au sein des groupes de travail du Conseil, et le Conseil «Justice et affaires intérieures» a avalisé en 2008 les progrès réalisés. Les discussions que les groupes de travail ont consacrées à la proposition ont permis de dégager un consensus sur la plupart de ses dispositions.

N'ayant pas encore été adoptée par le Conseil lors de l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, la proposition de la Commission est devenue obsolète. Le «programme de Stockholm - Une Europe ouverte et sûre qui sert et protège les citoyens»[3] demande à la Commission de présenter une proposition concernant l'utilisation des données PNR aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité (ci-après les «infractions graves»), ainsi que des enquêtes et des poursuites en la matière.

Dans le cadre de l'analyse d'impact de 2007, la Commission a consulté toutes les parties intéressées. À la suite de l'adoption de la proposition de 2007 de la Commission, toutes les parties intéressées - dont le Parlement européen, le groupe «Article 29» sur la protection des données, le contrôleur européen de la protection des données, l'Agence des droits fondamentaux et les associations de compagnies aériennes - ont publié des avis à son sujet. Le présent rapport a pour objet d'étudier la possibilité d'adopter une nouvelle proposition destinée à remplacer celle de 2007, conformément aux dispositions du traité de Lisbonne et aux procédures qu'il prévoit. Il vise à répondre aux critiques soulevées par les parties intéressées et à tenir compte de tous les faits nouveaux et de l'expérience acquise depuis 2007.

2. DÉFINITION DU PROBLÈME

2.1. La menace que représentent le terrorisme et la grande criminalité

Dans l'Union européenne et d'autres régions du monde, la dernière décennie a été marquée par une propagation de la criminalité transfrontière. Selon le recueil européen de statistiques relatives à la criminalité et à la justice pénale, 143 948 infractions pénales par tranche de 100 000 habitants ont été dénombrées en 2007 dans les États membres de l'UE (à l'exception de l'Italie et du Portugal pour lesquels des données n'ont pas été communiquées), ce nombre allant de 14 465 en Suède à 958 à Chypre. L'évaluation, effectuée en 2009 par Europol, de la menace que représente la criminalité organisée dans l'UE a révélé que la plupart des menaces relevant de la criminalité organisée revêtent une dimension internationale et que la majorité des infractions graves commises par des groupes criminels organisés impliquent des déplacements internationaux.

Le terrorisme constitue actuellement l'une des plus grandes menaces pour la sécurité, la paix, la stabilité, la démocratie et les droits fondamentaux. La menace terroriste ne se cantonne pas à certaines zones géographiques. S'il constate une régression du terrorisme dans l'UE en 2009, le rapport 2010 d'Europol sur la situation et les tendances du terrorisme en Europe souligne que cette menace demeure réelle et sérieuse. La plupart des campagnes terroristes, et

---

1 COM(2007) 654.
2 SEC(2007) 1453.
3 Document nº 17024/09 du Conseil du 2.12.2009.

en particulier ce qu'Europol appelle le «terrorisme islamiste, revêtent un caractère transnational.

2.2. Les données PNR et leurs utilisations

Les données PNR sont utilisées depuis plusieurs années, essentiellement par les services douaniers et répressifs de par le monde. Dans les domaines policier et judiciaire, elles peuvent être utilisées:

- **en mode réactif:** dans le cadre d'enquêtes, de poursuites, du démantèlement de réseaux après qu'une infraction a été commise. Pour permettre aux services répressifs de remonter suffisamment loin dans le temps, il est nécessaire de prévoir à cet effet une durée de conservation des données par ces services qui soit proportionnée;
- **en temps réel:** avant l'arrivée ou le départ de passagers dans le but de prévenir une infraction ou de surveiller ou d'arrêter des personnes avant qu'une infraction soit commise ou parce qu'une infraction a été commise ou est en train de l'être. Dans de tels cas, les données PNR sont particulièrement utiles pour établir des comparaisons, d'une part, avec des critères d'évaluation préétablis afin d'identifier des personnes jusqu'alors «inconnues» des services répressifs et, d'autre part, avec diverses bases de données de personnes et objets recherchés;
- **en mode proactif:** pour l'analyse et la définition de critères d'évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ. Pour effectuer cette analyse de pertinence pour les infractions terroristes et les infractions graves, il est nécessaire de prévoir une durée de conservation des données par les services répressifs qui soit proportionnée.

Ces obligations légales doivent être imposées aux transporteurs aériens pour les raisons exposées ci-après.

Premièrement, les données PNR permettent aux services répressifs d'identifier des personnes auparavant «inconnues» d'eux, c'est-à-dire jusque-là non soupçonnées de participation à une infraction grave ou à un acte de terrorisme, mais dont l'analyse des données indique qu'elles peuvent être impliquées dans une infraction de cette nature et qu'elles devraient donc être soumises à un examen approfondi par les autorités compétentes. L'identification de ces personnes aide les services répressifs à prévenir et à détecter les infractions graves, y compris les actes de terrorisme. À cet effet, lesdits services doivent utiliser les données PNR, d'une part, en temps réel, pour les analyser au regard de critères d'évaluation préétablis, qui indiquent les personnes jusque-là «inconnues» devant faire l'objet d'un examen approfondi et, d'autre part, d'une manière proactive aux fins de l'analyse et de la définition de critères d'évaluation.

Par exemple, une analyse de données PNR peut donner des indications sur les itinéraires les plus empruntés pour la traite des êtres humains ou le trafic de drogue, autant d'éléments qui peuvent être intégrés dans les critères d'évaluation. La confrontation en temps réel des données PNR à ces critères permet de prévenir ou de détecter des infractions. Un État membre a fourni un exemple concret concernant la traite des êtres humains: dans cette affaire, l'analyse des données PNR a permis de démasquer un groupe de passeurs qui empruntaient toujours le même itinéraire. Ils utilisaient des documents falsifiés pour procéder aux formalités d'enregistrement sur un vol intra-UE et utilisaient des documents authentiques pour procéder, simultanément, aux formalités d'enregistrement sur un autre vol à destination d'un pays tiers. Une fois dans la salle d'attente de l'aéroport, ils embarquaient sur le vol intra-UE. Sans les données PNR, il aurait été impossible de démanteler ce réseau de traite des êtres humains.

Une utilisation à la fois proactive et en temps réel des données PNR permet donc aux services répressifs de contrer la menace que représentent la grande criminalité et le terrorisme sous un angle différent, par rapport au traitement d'autres catégories de données à caractère personnel. Comme expliqué ci-dessous, le traitement de données à caractère personnel accessibles aux services répressifs dans le cadre d'instruments de l'UE actuels et futurs, tels que la directive relative aux informations préalables sur les passagers[4], le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II), ne donne pas aux services répressifs la possibilité d'identifier des suspects «inconnus», comme le permet l'analyse de données PNR.

Deuxièmement, après la commission d'une infraction, les données PNR aident les services répressifs à prévenir et à détecter d'autres infractions graves, dont des actes de terrorisme, et à enquêter sur celles-ci et à poursuivre leurs auteurs. À cet effet, les services répressifs doivent utiliser les données PNR en *temps réel*, pour les confronter à diverses bases de personnes «connues» et d'objets recherchés. Ils doivent également en faire un usage *réactif*, pour rassembler des preuves et, au besoin, trouver d'éventuels complices et démanteler des réseaux criminels.

Par exemple, les informations liées à une carte de crédit qui font partie des données PNR peuvent permettre aux services répressifs d'identifier une personne et d'établir l'existence de liens entre celle-ci et un délinquant ou une organisation criminelle qu'ils connaissent. Un État membre a cité un exemple relatif à un vaste réseau de traite des êtres humains et de trafic de drogue entre un État membre et des pays tiers. Des cartels importaient de la drogue dans plusieurs régions d'Europe. Ils faisaient appel à des personnes, elles-mêmes victimes de la traite, qui avalaient la drogue. Les données PNR ont permis leur identification car ils avaient acheté leurs billets avec des cartes de crédit volées. Des arrestations ont ensuite eu lieu dans l'État membre concerné. Un critère d'évaluation a été défini sur cette base, qui a à son tour permis plusieurs arrestations dans d'autres États membres et dans des pays tiers.

Enfin, l'examen des données PNR avant l'arrivée des passagers permet aux services répressifs de procéder à une évaluation et de ne contrôler étroitement que les personnes les plus susceptibles de représenter une menace pour la sécurité, sur la base de critères d'évaluation objectifs et de l'expérience acquise. Cela facilite le déplacement de tous les autres passagers et réduit le risque qu'ils soient soumis à un contrôle fondé sur des critères illégaux, tels que la nationalité ou la couleur de peau, que les services répressifs, et notamment les douaniers et gardes-frontières, peuvent à tort associer à un risque pour la sécurité.

Des accords en matière de transmission de données PNR dans le cadre de la lutte contre le terrorisme et la criminalité transnationale organisée ont été conclus entre l'UE et les États-Unis, le Canada et l'Australie. D'autres pays tiers solliciteront vraisemblablement à l'avenir la transmission de données PNR par les transporteurs aériens qui assurent des vols au départ de l'UE.

Le Royaume-Uni, la France et le Danemark ont déjà adopté des dispositions de droit primaire prévoyant la saisie et l'utilisation de données PNR. Ces mesures nationales divergent à plusieurs égards et lorsque ces États membres auront adopté le cadre réglementaire complet, d'autres divergences apparaîtront vraisemblablement. Étant donné que d'autres États membres élaborent actuellement des instruments législatifs relatifs aux données PNR, jusqu'à 27 systèmes sensiblement différents pourraient voir le jour, ce qui se traduirait par des degrés inégaux de protection des données, des lacunes en matière de sécurité, des hausses de coûts et une insécurité juridique pour les transporteurs aériens.

---

[4] Directive 2004/82/CE du 29 avril 2004.

2.3. Le principe de subsidiarité: un droit d'action pour l'UE

Le droit d'action de l'UE dans ce domaine est consacré par les articles 82 et 87 du titre V du traité sur le fonctionnement de l'Union européenne. Puisque la plupart des infractions graves, telles que le trafic de drogue ou la traite des êtres humains, impliquent à un moment donné des déplacements internationaux, il est primordial que les autorités recueillent, traitent et échangent des données PNR pour accroître la sécurité intérieure de l'Union. Vu la libre circulation des personnes dans l'espace Schengen, il est indispensable que tous les États membres aient recours aux données PNR pour éviter toute lacune en matière de sécurité. Par ailleurs, une action au niveau de l'UE permettra d'harmoniser les dispositions relatives à la protection des données, de réduire les coûts et d'accroître la sécurité juridique pour les transporteurs.

3. OBJECTIFS

3.1. Objectifs politiques

L'objectif général est de renforcer la sécurité intérieure de l'UE, tout en respectant le droit à la protection des données à caractère personnel et d'autres droits fondamentaux, parallèlement à la poursuite des objectifs spécifiques suivants.

(1) Prévenir et réduire les activités terroristes et les autres infractions graves, en adoptant une approche globale de l'utilisation des données PNR et en évitant toute lacune en matière de sécurité.

(2) Garantir le respect du droit des personnes à la protection des données à caractère personnel les concernant lors de la collecte et du traitement des données PNR, en facilitant l'échange des données PNR entre les autorités compétentes et en s'assurant que l'accès à ces données est limité au strict nécessaire.

(3) Assurer aux transporteurs une sécurité juridique et réduire les coûts qu'ils supportent, en rapprochant les diverses exigences juridiques et techniques qui leur sont imposées.

3.2. Considérations relatives aux droits fondamentaux

Dans l'analyse d'impact, les incidences sur les droits fondamentaux ont été appréciées au regard de la «check-list droits fondamentaux», ainsi que le prévoit la stratégie de la Commission pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne[5].

L'utilisation des données PNR affecterait les droits fondamentaux à la protection de la vie privée et à la protection des données à caractère personnel. Elle pourrait être subordonnée à des restrictions et à des conditions, pour autant que l'atteinte à ces droits soit «conforme à la législation» et «nécessaire dans une société démocratique». Les mesures proposées étant destinées à lutter contre le terrorisme et d'autres infractions graves, elles serviraient un objectif d'intérêt général susceptible de justifier ces restrictions, sous réserve du respect du principe de proportionnalité.

Chacune de ces mesures relèverait du champ d'application du chapitre 5 du titre V du TFUE, relatif à la coopération policière. 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

[5] COM(2010) 573 du 19 octobre 2010.

matière pénale[6] ne s'appliquerait qu'aux volets des mesures proposées faisant intervenir une transmission de données à caractère personnel entre États membres; un vide subsisterait donc pour les données à caractère personnel traitées au seul niveau national. Il n'existe actuellement aucune réglementation de l'UE qui encadre le traitement de données à caractère personnel à l'échelon national. La solution la plus appropriée consisterait à faire en sorte que toute mesure prévoie, en matière de protection des données, des garanties qui soient conformes à la décision-cadre 2008/977/JAI. Un niveau uniforme de protection des données à caractère personnel serait ainsi assuré.

Il est indispensable de prévoir un délai proportionné durant lequel les autorités compétentes conservent les données. Quant au mode de transmission des données par les transporteurs, le système «push» présente d'indéniables avantages par rapport au système «pull», raison pour laquelle il devrait s'appliquer à toutes les transmissions.

En ce qui concerne les critiques relatives à l'établissement de profils, le droit de l'Union en matière de protection des données confère à chacun le droit de ne pas être l'objet d'une décision produisant des effets juridiques préjudiciables à son égard ou l'affectant gravement et prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. Les décisions individuelles automatisées devraient être vérifiées intégralement, confirmées par une personne et comporter des dispositions permettant à l'intéressé de faire valoir son point de vue.

4. OPTIONS STRATÉGIQUES

L'analyse d'impact examine quatre options principales.

Option A. S'abstenir de réglementer la question au niveau de l'UE et maintenir le statu quo.

Option B. Options relatives à la structure du système PNR:

B.1: collecte et traitement décentralisés des données par les États membres; B.2: collecte et traitement centralisés des données au niveau de l'UE.

Option C. Options relatives à la limitation des finalités:

C.1: accès limité aux infractions terroristes et aux infractions graves; C.2: accès autorisé pour les infractions terroristes et les infractions graves, ainsi qu'aux fins d'autres objectifs stratégiques.

Option D. Options relatives aux modes de transport:

D.1: transporteurs aériens uniquement; D.2: transporteurs aériens, maritimes et ferroviaires.

Option E. Coopération volontaire/renforcée. Cette option consistant à encourager la coopération entre États membres dans ce domaine a été rejetée au stade initial.

5. COMPARAISON DES OPTIONS ET DE LEURS IMPACTS

Les options ont été évaluées au regard de leur impact en termes de renforcement de la sécurité dans l'UE, de renforcement de la protection des données à caractère personnel, de coûts pour

[6] 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.

les pouvoirs publics, de coûts pour les transporteurs, de concurrence dans le marché intérieur, de relations avec les pays tiers et de promotion d'une approche globale.

L'option A consistant à maintenir le statu quo présente des avantages limités pour le renforcement de la sécurité de l'UE, tout en ayant des effets négatifs en ce sens qu'elle causerait des difficultés administratives et engendrerait des coûts résultant de la coexistence de nombreux systèmes nationaux divergents.

Quant à l'option B, la collecte décentralisée des données (option B1) présente des avantages en termes d'amélioration de la sécurité de l'UE par rapport à la collecte centralisée (option B2). L'option B2 risquerait fortement d'être un échec car une coopération adéquate entre les États membres ne peut être garantie et, au niveau pratique, le système aurait un fonctionnement lourd et onéreux. L'option B1 serait toutefois plus chère que l'option B2, mais ses avantages sur le plan de la sécurité l'emportent sur ses inconvénients en termes de coûts.

En ce qui concerne la limitation des finalités, l'option C2 comporte quelques avantages pour la sécurité par rapport à l'option C1, mais elle implique une atteinte nettement plus importante à la protection des données et des coûts plus élevés que l'option C1. L'option C2 consistant à élargir l'utilisation des données PNR pour poursuivre d'autres finalités semble disproportionnée à ce stade.

Pour ce qui est des modes de transport, l'option D2 est avantageuse en termes de sécurité par rapport à l'option D1, car elle inclurait d'autres modes de transport et davantage de passagers, mais elle porterait plus grandement atteinte à la protection des données et serait plus coûteuse que l'option D1, selon laquelle la mesure s'appliquerait exclusivement aux transporteurs aériens. L'option D2 prévoyant d'élargir la portée de la mesure aux transporteurs maritimes et ferroviaires apparaît prématurée, tout au moins à ce stade.

6. OPTION PRIVILÉGIÉE

La meilleure option à ce stade (une combinaison des options B1, C1 et D1) semble consister dans l'élaboration d'une nouvelle proposition législative applicable aux déplacements aériens, prévoyant une collecte décentralisée des données PNR aux fins de la prévention et de la détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites en la matière. Elle offrirait les meilleurs outils pour renforcer la sécurité au sein de l'Union, l'impact sur la protection des données étant limité au strict minimum et les coûts maintenus à un niveau acceptable.

Les coûts inhérents à l'option privilégiée ont été étudiés dans le cadre de l'analyse d'impact de 2007. Selon les calculs effectués en 2007, le coût global de l'option privilégiée pour les pouvoirs publics et les transporteurs se ventilerait comme suit:

<u>En ce qui concerne les pouvoirs publics, les estimations de coûts pour l'ensemble des États membres sont les suivantes</u>:

Coût de mise en place (non récurrent)	614 833 187 €
MAIS dans l'hypothèse d'un amortissement sur cinq ans	122 966 637 €
Frais de personnel annuels (récurrents)	11 686 749 €
Frais de maintenance annuels (récurrents)	61 483 319 €

<u>En ce qui concerne l'ensemble des transporteurs de l'UE, ces coûts sont les suivants</u>:

Coût d'installation du système PUSH (non récurrent)	11 647 116 €

MAIS dans l'hypothèse d'un amortissement sur cinq ans 2 329 423 €

Coûts de transmission PUSH deux fois par passager (récurrents) 2 250 080 €

Frais de personnel et de maintenance (récurrents) 5 435 321 €

En 2008, la Commission a publié un appel d'offres pour la réalisation d'une étude sur la mise en place d'un réseau PNR au niveau de l'UE. Le rapport qui en a résulté, intitulé «Study on ways of setting up an EU network on exchange of Passenger Name Record (PNR) data for law enforcement purposes»[7], a été publié en 2009 et contient une nouvelle évaluation des coûts.

<u>En ce qui concerne les pouvoirs publics, les estimations de coûts pour l'ensemble des États membres sont les suivantes:</u>

Coût de mise en place (non récurrent) 221 000 000 €

MAIS dans l'hypothèse d'un amortissement sur cinq ans 44 200 000 €

Frais de personnel annuels (récurrents) 11 686 749 €

Frais de maintenance annuels (récurrents) 61 483 319 €

<u>En ce qui concerne l'ensemble des transporteurs, ces coûts sont les suivants:</u>

Coût d'installation du système PUSH (non récurrent)

100 000 € * 120 transporteurs établis dans l'UE = 12 000 000 €

100 000 € * 80 transporteurs non établis dans l'UE = 8 000 000 €

MAIS dans l'hypothèse d'un amortissement sur cinq ans 4 000 000 €

Coûts de transmission PUSH deux fois par passager (récurrents)

33 500 € par compagnie aérienne par an * 120 transporteurs * 3 connexions * 2 PUSH 24 120 000 €

Frais de personnel et de maintenance (récurrents) 6 240 000 €

Les chiffres de 2009 indiquent une baisse des frais de mise en place d'un système PNR de l'UE pour les pouvoirs publics, mais une hausse pour les transporteurs par rapport au calcul effectué en 2007. En réalité, les coûts se situeront entre ces deux estimations et, au moins en ce qui concerne les transporteurs, seront plus proches des évaluations de 2007 qui reposent sur les prix de marché directement fournis par les transporteurs.

Même si l'on tient compte des résultats très élevés des calculs de 2009, à supposer que les transporteurs décident de répercuter leurs frais sur les passagers, le surcoût qui en résulterait serait inférieur à 0,10 EUR par billet, soit un montant négligeable par rapport au prix global du billet.

[7] Auteurs: Accenture et SITA.

7. SUIVI ET EVALUATION

Chaque État membre pourrait rédiger un rapport annuel sur la mise en place des systèmes. La Commission devrait évaluer le fonctionnement de la directive dans un délai de quatre ans à compter de son entrée en vigueur pour déterminer si l'utilisation des données PNR a permis d'atteindre les objectifs fixés, si les États membres ont rempli leurs obligations et si le système est une réussite.

La Commission devrait également envisager la possibilité d'étendre la mesure aux vols intra-UE. Cela permettrait de disposer d'une période transitoire et de tirer des enseignements du fonctionnement de la première directive sur les données PNR.