Note numéro 19
Juillet 2016

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

« Fichier » PNR : surveillance électronique de masse ou nouveau paradigme de la sécurité ?

Le 16 avril 2016, les Députés européens adoptaient par 463 voix contre 174[1] la directive dite « fichier PNR »[2] (*passenger name record*[3]) qui encadre la collecte et le partage des données à caractère personnel[4] des passagers du transport aérien. Le contenu de ce texte, par les débats qu'il a suscités, demeure encore très controversé en raison des enjeux touchant aux libertés publiques. En effet, l'utilisation des données des dossiers passagers (DP) a pour finalité entre autre de faciliter la mise en œuvre de techniques dite de profilage[5] à l'aide d'un système de traitement automatisé. À ce stade, nombre de détracteurs appellent à la vigilance, dénonçant l'avènement d'une société où la surveillance électronique de masse serait érigée en système. Les DP vont compléter la traçabilité du trajet réalisé par tout passager empruntant la voie aérienne. En effet, les compagnies aériennes collectent déjà des données dite API (*advanced passenger information*)[6]qui comprennent les données d'identification des passagers ou des membres de l'équipage, provenant du passeport ou d'un autre document de voyage ainsi que des informations générales concernant le vol.

De manière plus spécifique au transport aérien, les fortes réserves émises dans l'usage des données des DP porteraient notamment sur l'existence d'un risque avéré d'erreur manifeste d'appréciation vis-à-vis du comportement d'un individu qui serait a priori suspect en raison des déplacements réalisés et du profil qu'il présente par au regard des résultats issus des données à caractère personnel transmis par une compagnie de transport aérien. La crainte d'une surveillance de masse et d'atteintes à la vie privée expliquent en grande partie que la directive PNR ait été bloquée au stade de la discussion depuis 2011 au Parlement européen.

Les attentats de Paris et de Bruxelles ont eu pour premier effet une demande accrue de sécurité de la part des opinions publiques choquées. Cette inquiétude des populations a pesé sur la nécessité de faire aboutir les débats de fond. Cependant, en l'absence de visibilité sur la période d'entrée en vigueur du projet de Directive PNR, des États européens, comme la France, avaient déjà fait le choix de légiférer en cette matière. Le gouvernement français a mis à profit l'adoption de la loi de programmation militaire 2014-2019 pour prévoir dans son article 17[7]que les transporteurs aériens puissent recueillir et transmettre les données d'enregistrement relatives aux passagers des vols à destination et en provenance du territoire national en excluant les vols internes.

1 Cf Médiapart, *Feu vert du Parlement européen à la collecte des données PNR,* article de la rédaction publié le jeudi 14 avril 2016.

2 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) 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. La présente directive doit être transposée dans l'ordre juridique interne des États au plus tard le 25 mai 2018. http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0681&rid=1

3 Traduction : dossier du passager (DP) – Cf avis de la Commission d'enrichissement de la langue française – JO du 22/03/2016 – Texte n°70.

4 Art 4, 4) du règlement (UE) 2016/679 définit une donnée à caractère personnel comme : *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.*

5 Idem règlement supra, le profilage se définit à l'art. 4,4) comme : « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser et prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. »*

6 Traduction : renseignements préalables concernant les voyageurs (RPCV).

7 Cf Loi 2013-1168 du 23 décembre 2013 - art 17, repris dans l'art. L.232-7 du Code de la sécurité intérieure (CSI) – Le législateur a prévu que cet article est applicable jusqu'au 31 décembre 2017,anticipant ainsi sur la nécessité d'un délai raisonnable pour transposer la directive PNR dans le droit interne.

La présente note commentera le contenu des dispositions de la directive en s'attachant à mettre en évidencel'architecture générale et le rôle des différents acteurs privés et publics intervenants dans le processus d'exploitation des données des dossiers passagers (DP). Cette présentation effectuée, nous nous attacherons de mettre en évidence que ce texte veille au maintien de grands équilibres indispensables dans toute société démocratique organisée autour du principe de l'État de droit. Quatres annexes, dont deux issues *in extenso* de la directive, apportent un éclairage concret sur la nature des DP, la liste des infractions à prévenir et/ou à détecter grâce à ceux-ci. Les deux dernières annexes récapitulent sous la forme de tableaux l'encadrement juridique du traitement des données PNR ainsi que les modalités de partage de celles-ci dans le cadre de la coopération entre les États.

I – Une directive qui cherche à impliquer l'ensemble des agents et opérateurs du transport aérien.

Fruit d'un très large consensus, la directive 2016/681 a été adoptée par tous les États membres de l'Union européenne a l'exception du Danemark[8]. Cet État, a déclaré qu'il ne se sentait pas lié ni soumis à l'application du contenu de ce texte. A contrario, le Royaume-Uni et de l'Irlande[9] ont notifié leur souhait de participer pleinement à l'adoption et à l'application de cette directive.
La directive s'appuie essentiellement sur deux acteurs essentiels : les transporteurs aériens et les unités d'information passagers (UIP). Les premiers ont pour rôle de recueillir, stocker et transférer les données des DP mentionnées à l'annexe 1 de la directive et seulement celles-ci. Il convient de souligner que les données mentionnées étaient déjà collectées par les compagnies aériennes à des fins d'exploitation commerciale. De ce fait, les compagnies aériennes devraient être rapidement opérationnelles dans la gestion de ces mégadonnées[10].
La directive concerne en priorité les dossiers passagers en relation avec les vols extra-européen[11] sans toutefois exclure les vols intra-Union européenne[12] (UE). Ces DP sont par la suite transférés auprès d'une structure créée par chaque État, à compétence nationale, dénommée Unité d'Information des Passagers (UIP). Conséquence directe de l'application de l'article 17 de la LPM, l'UIP est entrée dans une phase opérationnelle[13] en France sous l'égide du ministre chargé des Douanes[14]. Cette UIP a la responsabilité de la gestion du traitement automatique de données à caractère personnel par l'intermédiaire du *"Système API-PNR France"*[15].
La directive propose une certaine souplesse aux États signataires en charge de la mise en oeuvre. Tout d'abord, le texte prévoit expressément que deux États membres ou plus peuvent, s'ils le désirent, mettre en place ou désigner une autorité unique en tant qu'UIP. Ainsi, toute coopération envisagée reste à la discrétion des États. Dans cette configuration, l'UIP commune serait implantée sur le sol d'un des États membres et agirait en conséquence comme une UIP nationale. Autre aspect laissé à l'initiative des États membres, la faculté d'étendre l'application de la directive PNR aux vols intra-Union européenne (Art. 2) permet à un État membre d'appliquer cette réglementation à la totalité des vols intra-UE ou seulement une partie de ceux qu'il aura sélectionnés de manière souveraine.
Les transporteurs aériens, en tant qu'opérateurs économiques, exercent une mission d'intérêt général par le fait de récolter et de transférer les DP énumérées en annexe1, à l'exclusion de

8 Cf considérant 40 de la directive.
9 Cf considérant 39 du texte supra.
10 Équivalent étranger de *big data* qui désigne « *des données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés »*. L'expression « données massives » est aussi employée. Cf Avis de la Commission générale de terminologie et de néologie, Journal officiel du 22 août 2014, texte n°89.
11 La directive définit « vol extra-européen »: *tout vol, régulier ou non, effectué par un transporteur aérien en provenance d'un pays tiers et devant attérir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers. (art.3.(2)*
12 La directive définit « vol intra-européen » : *tout vol, régulier ou non, effectué par un transporteur aérien en provenance du territoire d'un État-membre et devant atterir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers. (art 3.(3)*
13 Cf Le Parisien « *Roissy : les douanes vont pister les passagers suspects. »*http://www.leparisien.fr/roissy-en-france-95700/roissy-les-douanes-vont-pister-les-passagers-suspects-19-03-2015-4618147.php
14 Décret n°2014-1566 du 22 décembre 2014 – JO du 24 décembre 2014 – Texte n°30.
15 Décret n°2014-1095 du 26 septembre 2014 – JO du 26 septembre 2014 – Texte n°15.

toutes autres, à destination de l'UIP compétente. En cas de manquement à leurs obligations (ex : non transmission de données, non respect du format requis), chaque État membre aura à prévoir, au moment de la transposition de la directive dans leur ordre juridique interne, un régime de sanctions y compris financières. Selon les termes de l'article 14 de la directive : "*les sanctions prévues doivent être effectives, proportionnées et dissuasives."*

La directive PNR a vocation à évoluer à terme en fonction des enseignements qui seront tirés dans son application. En matière de complémentarité, les rédacteurs ont pris soin d'éviter que les dispositions du texte entrent en contradiction avec d'autres instruments juridiques éprouvés. Pour ce qui concerne la coordination avec lesdits instruments, la directive PNR se veut compatible avec les lignes directrices existantes de l'organisation de l'aviation civile internationale (OACI). Il s'agit en particulier d'adopter des formats de données reconnus de tous pour le transfert des données avec les protocoles correspondants. Cette directive exprime l'intention aussi d'être au maximum compatible avec les engagements antérieurs en vigueur qu'auraient contractés les États membres ou de l'Union avec des pays tiers. Seules les modalités d'échange d'informations devront répondre aux conditions prévues avec la directive PNR (tableau – Annexe III). S'agissant de l'orientation susceptible d'être donnée à la directive dans les années à venir, la Commission européenne procédera, au plus tard le 25 mai 2020, à un réexamen de tous les éléments du texte. À cette occasion, le futur rapport devrait évaluer, entre autre, la pertinence de faire figurer d'autres opérateurs économiques en lien avec les flux aériens tels que les agences et organisateurs de voyages. Ces opérateurs sont amenés, dans le cadre de leur activité, à proposer des services liés au voyage comme la réservation de vols. Ainsi, en impliquant pleinement le champ des opérateurs économiques dans la mission de sécurité des personnes et des biens, les instances publiques européennes et nationales montrent une volonté de faire de la donnée le noyau dur des futures politiques partenariales dans le domaine de la sécurité publique.

L'usage des données à caractère personnel comme celles des DP dans la prévention et la détection des infractions terroristes ou d'autres formes graves de criminalité exige en contre-partie des garanties pour la préservation des droits fondamentaux sans lesquelles nos sociétés basculeraient, selon l'expression retenue dans une résolution du Parlement européen, dans une forme d'État « ultrapréventif [16]».

II – <u>Une gouvernance des données régie sous le prisme de la maîtrise et du contrôle.</u>

La directive PNR 2016/681 organise une gouvernance des DP en cherchant à assurer la maîtrise et le contrôle de leur contenu tout au long d'un cycle d'emploi immédiat. Ce cycle se situe essentiellement entre la réservation du voyage jusqu'à l'accomplissement de celui-ci. Au-delà de ce cycle, les DP sont stockées pour une durée utile de 5 ans avant d'être effacées de manière définitive.

Cette gouvernance des DP fait transparaître une forme de principe de séparation des pouvoirs : d'un côté, des responsables de traitement (compagnies aériennes) strictement cantonnés dans leurs prérogatives de collecte et de transmission des DP dont la nature pertinente a été préalablement définie, en bout de ligne, un responsable de traitement (UIP), chargé d'analyser et d'exploiter les dites DP avec pour finalité la lutte et/ou la prévention d'une série d'infractions préalablement qualifiées. Cette approche fondée sur une recherche de séparation des pouvoirs est renforcée par ailleurs par la méthode technique d'envoi des DP retenue. Sur ce point, la directive PNR retient une méthode de transfert bien particulière que les compagnies aériennes

16« *estime que les programmes de surveillance constituent une nouvelle étape vers la mise en place d'un État "ultrapréventif", s'éloignant du modèle établi du droit pénal en vigueur dans les sociétés démocratiques, selon lequel toute atteinte aux droits fondamentaux d'un suspect nécessite l'autorisation d'un juge ou d'un procureur, en l'existence de soupçons raisonnables, et doit impérativement être régie par la loi, pour y substituer un mélange d'activités de répression et de renseignement avec des garanties juridiques floues et affaiblies, allant bien souvent à l'encontre des freins et contrepoids démocratiques et des droits fondamentaux, en particulier de la présomption d'innocence; rappelle à cet égard la décision de la Cour constitutionnelle fédérale allemande sur l'interdiction du recours au profilage préventif (präventive Rasterfahndung) en l'absence d'éléments démontrant la mise en péril d'autres droits importants et juridiquement protégés, selon laquelle une menace générale ou des tensions internationales ne suffisent pas à justifier de telles mesures »; Cf* Résolution du Parlement européendu 12 mars 2014, P.21, conclusions principales, paragraphe 12.
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0230+0+DOC+PDF+V0//FR

auront à adopter. Dans ses considérants, la directive rappelle l'existence de deux méthodes de transfert : « *pull*[17] » ou « *push*[18] ». À l'évidence, pour les instances européennes, la méthode « *push* » apporterait le plus de garantie en matière de protection des données à caractère personnel. L'avantage majeur de cette méthode réside dans le fait que l'autorité requérante (UIP) ne peut accéder aux systèmes de traitement automatique de données (STAD) des compagnies aériennes. Ces entreprises conservent ainsi le contrôle sur les données transmises. Ce principe de séparation entre celui qui collecte et transmet la donnée et celui qui l'analyse et l'exploite rappelle dans un autre contexte, le principe fondamental en France en matière de comptabilité publique de la séparation des ordonnateurs et des comptables[19]. Les données à l'instar des fonds monétaires, ont pour point commun un caractère sensible par les usages auxquels on peut les destiner. La transmission des données du dossier passager (DP) est rigoureusement encadrée dans une séquence chronologique que les compagnies aériennes sont tenues de respecter. Les sociétés transfèrent les DP d'un vol programmé au sein d'un échéancier contraint[20] : "*24 à 48 heures avant l'heure de départ programmée du vol et immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'ils ne peuvent plus embarquer ou débarquer."* Dans l'absolu, la directive mentionne que les transporteurs aériens transférent par deux fois les mêmes DP à l'UIP compétente. Pour éviter une répétition de cette opération pouvant être perçue comme dénuée de sens, chaque État membre a la faculté d'autoriser les transporteurs aériens à transférer à l'UIP seulement les DP qui nécessitent une actualisation. Hors de cette séquence chronologique, à la demande d'une UIP confrontée "*à une menace précise et réelle"*[21], les compagnies aériennes envoient au cas par cas des données PNR. Naturellement, ce genre d'envoi s'effectue conformément au droit national en vigueur. La directive encadre à la fois la période de conservation des données et leur dépersonnalisation. Sur le premier point, la durée de conservation des données PNR dans une base est fixée à une période de cinq ans. À l'issue de celle-ci, les données sont effacées de manière définitive[22]. Sur le second point, la durée des consultations « ouvertes » des DP par les personnels habilités de l'UIP ne peut pas excéder 6 mois à compter de leur réception. Au terme de ce délai, certains éléments[23]des données des DP doivent faire l'objet d'une mesure de dépersonnalisation. Cette opération consiste à masquer les éléments qui seraient de nature à rendre possible l'identification directe du passager. Malgré tout, le processus de dépersonnalisation des données demeure réversible. Il peut être levé au cas par cas pour toute demande dûment motivée et approuvée par une autorité judiciaire[24]. À ce stade, il convient de souligner que la mesure de dépersonnalisation des données PNR a constitué un des points de blocage auprès du Parlement européen. La France, ainsi que d'autres pays européen dans son sillage auraient souhaité que toute opération visant à dépersonnaliser des données DP intervienne au bout d'un an de conservation. À l'inverse, la tendance des députés européens se portait sur un trimestre au maximum[25]. À travers ce point de discussion, il ressort que la gouvernance des données à caractère personnel a été au coeur des préoccupations des travaux en raison de la sensibilité accrue de celles-ci. Sur un plan normatif, la directive PNR ne déroge à

17 Directive – Considérant n°16 - La méthode « pull » : *les autorités compétentes de l'État membre qui requièrent les données PNR peuvent accéder au système de réservation du transporteur aérien et en extraire (« pull ») une copie des données PNR requises.*

18 Art. 3. 7) de la directive «méthode push » : *la méthode par laquelle les transporteurs aériens transfèrent les données PNR énumérées à l'annexe I vers la base de données de l'autorité requérante.*

19 À l'origine de ce principe notamment l'Ordonnance Royale du 14 septembre 1822.

20Directive 2016/681 – Art.8 .3 a) et b)

21 Idem, Art. t8.5

22 Idem Art. 12. 1 et .4

23 L'art.12. 2. mentionne comme donnée à dépersonnaliser :

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR ;

b) l'adresse et les coordonnées ;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne ;

d) les informations « grands voyageurs »

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directment le passager auquel le PNR se rapporte ; et

f) toute donnée API qui a été recueillie.

24 Art. 12.3 combiné avec art 6.2. b)

25 Médiapart, *Accord européen sur un registre des passagers européens*, article de la rédaction publié le 5 décembre 2015.

aucun des textes fondamentaux adoptés par les instances européennes[26]. Chaque UIP est responsable de la mise en oeuvre d'une politique de protection des données à caractère personnel. Cette politique passe en premier lieu par une traçabilité des opérations de traitement réalisées par les agents de l'UIP[27]. L'ensemble des opérations figure dans un registre conservé pour une durée de cinq ans. En second lieu, une UIP a une obligation de notifier sans délai toute faille de sécurité découverte dans son STAD auprès de son autorité de contrôle nationale mais aussi des intéressés[28].
La directive 2016/681 est le fruit d'un compromis évolutif qui tend à la recherche d'un point d'équilibre permanent entre, d'un côté, le respect des libertés publiques et, de l'autre, les nécessités d'assurer, dans le cadre de la liberté de circulation, la sécurité des personnes et des biens. Le réexamen de la directive, tel que le prévoit son article 19, constitue au final une clause de sauvegarde générale des intérêts fondamentaux dont la philosophie réside dans le souci d'être en capacité de réagir promptement face à toute tentative insidieuse d'installer une surveillance électronique de masse organisée.

III – Le traitement des données : le nouveau paradigme des politiques de sécurité publique.

Les possibilités qu'offrent le traitement des données à caractère personnel, plus particulièrement celles provenant des DP, semblent introduire de fait un nouveau paradigme dans les stratégies des politiques publiques de sécurité. L'analyse spécifique des mégadonnées provenant des collectes des dossiers passagers (DP) ouvre des perspectives inédites dans le domaine de la prévention et de la détection de personnes potentiellement suspectes d'agissement à caractère criminels ou délictueux. Sur un plan plus technico-opérationnel, la directive encadre les finalités admises[29]dans le traitement automatisé des DP mais aussi les procédures qu'il convient d'adopter dans le partage des éléments analysés[30]. Le tableau mentionné à l'annexe III recense les trois finalités de traitement des DP autorisées par l'article 6 de la directive 2016/681. Dans ce volet, les instances européennes ont voulu que les UIP soient en mesure d'exploiter pleinement les DP en leur offrant la possibilité de réaliser des évaluations des passagers, de répondre au cas par cas aux demandes d'autorités compétentes et enfin d'analyser les DP sur la base de critères préétablis. Sur ce dernier point, la directive ne fournit aucune définition sur les critères préétablis admissibles. Tout au plus l'article 6.4 de ce texte rappelle-t-il que *« lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. »* L'analyse des DP sur des critères préétablis autorise a priori une amorce dans la mise en place de méthodes de police prédictive[31] (*predictive policing*) dans les emprises aéroportuaires. Sur ce point, les techniques de profilage apparaissent comme une des manifestations les plus tangibles du concept de police prédictive. Les méthodes dites de « prévision des délinquants » et a fortiori celles censées « prédire l'identité des auteurs de

26 Cf décision-cadre 2008/977/JAI, 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 L281 du 23.11.1995, p.31)
27 Art.13.6 : les opérations de traitement concernent *la collecte, la consultation, la communication et l'effacement des données*. Chacune de ces opérations mentionne la date, l'heure et dans la mesure du possible l'identité de l'agent qui a consulté ou comuniqué les données PNR et vers quels destinataires.
28 Art. 13.8 de la directive.
29 Art. 6.2
30 La directive distingue trois formes de partage : Art 9 *« Échange d'informations entre États membres »*, Art. 10 « *Conditions d'accès aux données PNR par Europol. »*, Art. 11 *« Transfert de données vers des pays tiers ».*
31 Cf à ce propos voir Le rapport d'évaluation, *« Predictive policing, The rôle of crime forecasting in law enforcement operations »*,Rand corporation,2015,p.xiii. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf (traduit de l'anglais) :
« Dans notre évaluation des services de police prédictive, nous avons constaté que les méthodes prédictives peuvent être divisées en quatre grandes catégories :
1. Méthodes pour prédire les crimes: ce sont les approches utilisées pour prévoir des lieux et des temps avec un risque accru de criminalité.
2. Méthodes de prévision des délinquants: Ce sont les approches utilisées pour identifier les personnes à risque comme délinquant à l'avenir.
3. Méthodes pour prédire l'identité des auteurs de violence: Ces techniques sont utilisées pour créer des profils qui correspondent précisément aux délinquants susceptibles de commettre des crimes spécifiques passés.
4. Méthodes pour prédire les victimes de crimes: semblables à ces méthodes qui mettent l'accent sur les délinquants, les lieux du crime, et les périodes de risque accru, ces approches sont utilisées pour identifier les groupes ou, dans certains cas, les personnes qui risquent d'être victimes d'actes criminels. »

violence » pourraient s'inscrire comme une hypothèse de départ dans les réflexions menées autour des techniques de profilage fondées sur des critères préétablis. Ces critères ouvrent le champ à l'expérimentation d'algorithmes[32] à des fins prédictives, seuls outils capables de traiter des données massives. La valorisation des résultats issus des analyses des données PNR ne peut gagner en efficience sans le développement d'une politique d'échange d'informations entre les États. Sur les conditions du partage des données, les articles 9,10 et 11 de la directive prennent le soin de distinguer l'échange entre États membres, l'accès aux DP par Europol ainsi que le transfert de celles-ci vers des pays tiers.

Le tableau figurant en annexe IV récapitule les différents cas de figure et les conditions qui s'y attachent. Ce texte, sans pour autant entraver la bonne marche de la coopération policière et pénale, veille toutefois à se prémunir de risques de contournement par rapport aux objectifs et aux finalités légitimes du traitement des DP. Ces trois cadres juridiques décrivent précisément les conditions de transfert des DP et veillent à assurer une traçabilité des actes réalisés dont l'UIP en est la garante.

Véritable « gardien »[33] des DP, l'UIP dispose d'un pouvoir d'usage, de contrôle et de direction de celles-ci. À ce titre, l'UIP est susceptible d'engager sa responsabilité dans les opérations qu'elle réalise sous le double regard des autorités de contrôle nationale[34] et du délégué[35] à la protection des données de l'État membre. Plus que jamais, le traitement de la donnée est au coeur de la fonction d'anticipation. Dans son sillage, les technologies d'essence prédictive sont une des manifestations du paradigme des politiques de sécurité publique.

Conclusion.

L'utilisation des données, plus particulièrement celles issues des DP, annonce une nouvelle rupture dans les politiques de sécurité publique. En 2011, le philosophe Éric SADIN[36] soulignait que l'ère du numérique accèlere l'entrée de notre société vers une quête d'anticipation de plus en plus forte. À ce titre, la révolution numérique influe de manière notable sur la vision traditionnelle du contrôle d'un territoire. En effet, un mouvement de fond des politiques de sécurité publique est en train de s'opérer en privilégiant davantage une approche de contrôle des flux des personnes et des biens que la seule approche plus conventionnelle du maillage du territoire. Ce nouveau paradigme avait déjà été expliqué par le philosophe Michel Foucault lors d'une de ses leçons au Collège de France, plus particulièrement à travers son concept du dispositif de sécurité[37]. Selon lui, il ne s'agirait plus de fixer et marquer le territoire mais plutôt de « *laisser faire les circulations, contrôler les circulations, trier les bonnes et les mauvaises, faire que ça bouge toujours, que ça se déplace sans cesse, que ça aille perpétuellement d'un point à un autre, mais d'une manière telle que les dangers inhérents à cette circulation en soient annulés*[38]*. »* Les techniques humaines comme l'évaluation comportementale[39] associées aux nouvelles technologies de sécurité comme le profilage et la police prédictive constituent dans l'ère dite de la société de l'anticipation une des voies envisagées pour anhiler les modes d'action terroristes notamment dans les aéroports.

---

32 « *Ensemble des régles opératoires propres à un calcul ou à un traitement informatique, définies en vue d'obtenir un résultat déterminé* » Définition http://gdt.oqlf.gouv.qc.ca/Resultat.aspx, Institut canadien des comptables agréés en 2006.

33 La jurisprudence de la Cour de cassation qualifie de gardien, celui qui a un pouvoir d'usage, de contrôle et de direction sur la chose (Cf Ch civ de la Cour de cassation, *arrêt Franck,* 2 décembre 1941).

34 Cf Art.15.1 à 4, ce rôle en France est naturellement dévolu à la CNIL qui dispose d'un pouvoir d'inspection et d'audit de sa propre initiative ou en se fondant sur une réclamation.

35. Nommé par l'UIP, il n'en demeure pas moins que l'Art.5.2. de la Directive enjoint les États membres de les doter « *des moyens pour accomplir leurs missions, conformément au présent article, de manière effective et en toute indépendance. »*

36 Auteur de *La société de l'anticipation, Le web précognitif ou la rupture anthropologique inculte*, Coll. Essais, 224 p ; septembre 2011. http://ericsadin.org/node/20 « *L'ambition contemporaine et prométhéenne à vouloir anticiper le plus exactement la marche des choses caractérise le renseignement du XXIe siècle ; dimension qui désormais s'étend aux champs économiques, juridiques, thérapeutiques, aux relations entre les personnes… La Société de l'anticipation analyse l'émergence d'une socialité dotée de pouvoirs techniques vertigineux, qui cherche à sécuriser et à optimiser son cours par une maîtrise maintenant possible de l'avenir, modifiant progressivement nos rapports historiques à l'espace, au temps, et aux autres ».*

37 Auteur de : *sécurité, territoire, population, cours au Collège de France. 1977-1978*, Hautes études, EHESS. GALLIMARD, SEUIL, 2004, P.13 et suivantes. Michel Foucault dégage 4 traits majeurs lorsqu'il évoque les dispositifs de sécurité : les espaces de sécurité, l'étude du problème du traitement de l'aléatoire, l'étude de la forme de normalisation spécifique à la sécurité qu'il différencie nettement avec la normalisation disciplinaire, l'existence d'une corrélation entre la technique de sécurité et la population comme objet et sujet de ces mécanismes.

38 Idem supra P.67

39 L'évaluation comportementale consiste selon les termes du décret « en une observation des personnes, accompagnée éventuellement de l'engagement d'une conversation, visant à détecter les personnes susceptibles de présenter un risque pour la sûreté de l'aviation civile. » Cf décret 2016-528 du 27 avril 2016 relatif à l'évaluation du comportement des personnes au sein d'un aérodrome ,JO du 30/04/2016, texte n°5.

ANNEXE I

Données des dossiers passagers (DP) telles qu'elles sont recueillies par les transporteurs.

1. Code repère du dossier passager
2. Date de réservation / d'émission du billet
3. Date(s) prévue(s) du voyage
4. Nom(s)
5. Adresse et coordonnées (numéro de téléphone, adresse électronique)
6. Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation
7. Itinéraire complet pour le PNR concernés
8. Informations « grands voyageurs »
9. Agence de voyages/agent de voyages
10. Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation
11. Indications concernant la scission/division
12. Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée)
13. Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix
14. Numéro du siège et autres informations concernant le siège
15. Informations sur le partage de code
16. Toutes les informations relatives aux bagages
17. Nombre et autres noms de voyageurs figurant dans le PNR
18. Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée)
19. Historique complet des modifications des données PNR énumérées aux points 1 à 18.

ANNEXE II

Liste des infractions visées à l'article 3, point 9

1. Participation à une organisation criminelle
2. Traite des êtres humains
3. Exploitation sexuelle des enfants pédopornographie
4. Trafic de stupéfiants et de substances psychotropes
5. Trafic d'armes, de munitions et d'explosifs
6. Corruption
7. Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union
8. Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro
9. Cybercriminalité
10. Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées
11. Aide à l'entrée et au séjour irréguliers
12. Meurtre, coups et blessures graves
13. Trafic d'organes et de tissus humains
14. Enlèvement, séquestration et prise d'otage
15. Vol organisé ou vol à main armée
16. Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art
17. Contrefaçon et piratage de produits
18. Falsification de documents administratifs et trafic de faux
19. Trafic de substances hormonales et d'autres facteurs de croissance
20. Trafic de matières nucléaires et radioactives
21. Viol
22. Infractions graves relevant de la Cour pénale internationale
23. Détournement d'avion/de navire
24. Sabotage
25. Trafic de véhicules volés
26. Espionnage industriel.

Note CREOGN n°19 - Annexe III – Traitement des données PNR prévu par l'article 6 de la Directive 2016/681.

RÔLE DE L'UIP **Nota : L'UIP efface immédiatement et de façon définitive dès réception les données autres que celles énumérées à l'annexe 1 de la Directive.**			
Finalités de traitement	**Objectifs**	**Modalités**	**Observations**
Réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu pour celui-ci. (Art.6.2.a)	**Identifier les personnes pour lesquelles est requis un examen plus approfondi compte-tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.**	**L'évaluation des passagers avant leur arrivée ou leur départ peut se réaliser soit par la confrontation des données PNR aux bases de données utiles (interrogation des fichiers judiciaires ou administratifs) soit au regard de critères préétablis** **Initiative de l'UIP ou examen requis à la demande des autorités compétentes (art 7.) ou Europol dans les limites de ses attributions.**	**En cas de concordance positive révélée par un STAD, procéder à un réexamen de la situation individuelle du passager concerné par des moyens non automatisés avant de prendre toute mesure sur le fond en vertu du droit national.** **Aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative ne peut être prise sur la seule base du traitement automatisé de données. PNR (Art. 7.6)**
Répondre au cas par cas aux demandes dûments motivés sur des motifs suffisants des autorités compétentes. (Art. 6.2.b)	**Évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci**	**Évaluation réalisée au regard de critères préétablis (ciblés, proportionnés et spécifiques) et non discriminatoires.**	**Critères fixés et réexaminés à intervalles réguliers.** **Lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.**
Analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées supra au cas par cas. (Art. 6.2.c)	**Identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.**	**Traiter les données PNR au regard de critères préétablis.**	**Interdiction d'utiliser des critères par nature discriminatoires (idem ci-dessus**

Note CREOGN N°19 - Annexe IV – Modalités de partage des données – Articles 9, 10 et 11 de la Directive 2016/681				
Cadres du partage	**Cas d'espèce**	**conditions**	**Conduite à tenir**	**Observation**
Article 9 : échange d'information entre États Membres	**Personne identifiée (Art.9.1) par une UIP dans une des situations évoquées à l'article 6.2 faisant suite soit :** a) à une évaluation, b) à une réponse à une demande (cas par cas), c) à un résultat d'analyse de données PNR sur la base de critères préétablis	- Personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité, - Le transfert des données s'effectue au cas par cas. - Nota : Si le résultat du traitement des données provient d'un STAD, obligation préalable avant tout transfert d'un réexamen individuel par des moyens non automatisés. Cf Art. 9.1, 6.2 et 6.6.	Transmission d'UIP au(x) UIP correspondante()s de toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de celle-ci	Les UIP des États membres destinataires transmettent les informations reçues à leurs autorités compétentes Cf art.6. 6 (nécessité préalable d'un réexamen individuel par des moyens non automatisés).
	Demande d'une UIP à une autre UIP (Art.9.2) : - De communication de données non dépersonnalisées (Cf Art12.2), - Du résultat d'analyses de ces données suite à une évaluation (cas supra Art. 6.2 a)	- Demande dûment motivée, - Dans un des cas spécifiques suivant : 1 – Prévention ou détection d'infractions terroristes, 2 – formes graves de criminalité, 3 – d'enquêtes ou de poursuites d'enquêtes en la matière.	Transmission des informations par l'UIP requise dès que possible. (Art.9.2). **<u>Nota</u>** : Si les données PNR ont été dépersonnalisées, transmission de celles-ci si existence d'un motif raisonnable de croire que celà est nécessaire aux fins visées à l'Art. 6.2. b + autorisation de l'autorité judiciaire ou autre autorité nationale compétente (Art.12.3. b)	La demande peut-être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments (Art.9.2).
	Demande d'une autorité compétente d'un État membre directement à une UIP d'un autre État membre. (Art.9.3)	- Cas d'urgence, - Demande motivée, - Application des dispositons de l'article 9.2 (Cf idem conduite à tenir dans le cas d'une demande d'une UIP à une autre UIP)	Si transmission accordée, **<u>envoie systématique d'une copie</u>** de la demande à l'UIP de l'État membre requérant.	**<u>Dans tous les autres cas</u>**, les autorités compétentes canalisent leurs demandes par l'intermédiaire de l'UIP de leur propre État membre.
	Demande à titre exceptionnel. (Art.9.4)	- Infractions terroristes ou formes graves de criminalité, - Pour répondre à une menace précise et réelle, - Au cas par cas.	L'UIP sollicitée examine si les conditions de recevabilité sont réunies et décide de la suite à donner.	Si demande accordée, transmission d'UIP requise à UIP requérante.

Cadres du partage	Cas d'espèce	Conditions	Conduite à tenir	Observations
Article 10 : conditions d'accès aux données PNR par Europol	Demande aux UIP des États membres de : - Données PNR ou, - Le résultat du traitement de ces données. (Art.10.1.)	- Dans la limite de ses compétences, - Pour l'accomplissement de ses missions. (Art.10.1.)	L'UIP sollicitée examine si les conditions de recevabilité sont réunies et décide de la suite à donner.	Europol informe le délégué à la protection des données de chaque échange d'informations. (Art.10.3.) Les échanges d'information ont lieu par l'intermédiaire de SIENA (**Secure Information Exchange Network Application)**, Application sécurisée d'échange d'information en réseau . Utilisation pour la demande et l'échange des informations de la langue en vigueur dans cette structure.(Art.10.4.) (Cf décision 2009/371/JAI)
	Demande électronique ***au cas par cas*** de transmission de données PNR ou du résultat de traitement de ces données. (Art.10.2.)	- Présentation de la demande : - Dûment motivée, - Strictement nécessaire au soutien et au renforcement de l'action des États membres, - Dans une des situations suivantes : 1 – Prévention ou détection d'une infraction terroriste spécifique, 2 – Forme grave de criminalité spécifique, 3 – Conduites d'enquête en la matière, 4- Entre dans le champ de la compétence d'Europol au regard de la décision 2009/371/JAI[40]		

40 Décision du 6 avril 2009 portant création de l'Office européenn de police (Europol)

Note N°19 CREOGN, fin Annexe IV.				
Cadre du partage	**Cas d'espèce**	**Conditions**	**Conduite à tenir**	**Observations**
Article 11 : Transfert de données vers des pays tiers.	**Uniquement au cas par cas.** La directive distingue le transfert de données en situation normale et lors de circonstances exceptionnelles consécutives en l'absence d'accord préalable de l'État membre.	**<u>Situation normale</u> :** - Données PNR et le résultat de leur traitement, - Uniquement celles conservées par l'UIP sous le régime des dispositions de l'Art.12. de la Directive. - Conditions de l'Art.13 de la décision-cadre 2008/977/JAI[41] sont remplies. - Le transfert est nécessaire aux fins : 1/Prévention ou détectiond'infractions terroristes, 2 – formes graves de criminalité, 3 – d'enquêtes ou de poursuites d'enquêtes en la matière. - Accord exprès de l'État membre concerné + conditions identiques à l'Art.9.2 de la Directive (Cf1er tableau)	Appréciation souveraine de l'État membre.	Le transfert se fait que dans des conditions compatibles avec la présente Directive et la garantie du pays tiers de s'y conformer. (Art. 11.3) Chaque transfert de données PNR de la part d'un État membre vers un pays tiers donne lieu à l'information systématique du délégué à la protection des données de l'UIP de l'État membre. (Art.11.4.)
		<u>Circonstances exceptionnelles sans l'accord préalable de l'État membre</u> : - Données PNR seulement, - Répondre à une menace précise et réelle (infraction terroriste ou forme grave de criminalité) - l'Accord préalable ne peut être obtenu en temps utile.	L'UIP informe sans retard l'autorité chargée de donner son accord. Le transfert est dûment enregistré et soumis à une vérification ex-post.	

*

41 La décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dan le cadre de la coopération policière et judiciaire en matière pénale **<u>est abrogée à compter du 6 mai 2018</u>** par la Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infraction pénales, d'enquêtes et de pôursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.