Rapport Sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale (2002)

AVANT-PROPOS

1. Lors de sa 74e réunion, le Comité européen de coopération juridique (CDCJ) a adopté le mandat révisé du Groupe de projet sur la Protection des données (CJ-PD) pour 2001 et 2002. Le Comité des Ministres a approuvé par la suite ledit mandat, tel qu'il est décrit dans le document CJ-PD (2000) 3 rev 4, lors de sa 740e réunion. Le CJ-PD s'y voit convié à :

> *« examiner, avant la fin 2001, les incidences des principes de la protection des données, d'une part, sur la coopération judiciaire, d'autre part, sur la coopération policière en matière pénale, notamment, dans le cadre du Groupe de travail sur la protection des données et la coopération policière et judiciaire en matière pénale (CJ-PD/GT-CP). »*

2. Afin de déterminer et de définir plus clairement les sujets à traiter, en prenant en compte le fait que les échanges de données entre les instances judiciaires dans le cadre de la coopération judiciaire en matière pénal ne constituent qu'un aspect particulier du traitement de l'information et que ceci, par conséquent, ne couvre pas toutes les activités impliquant le traitement de données à caractère personnel dans le domaine judiciaire, le CJ-PD a décidé de modifier légèrement le nom du nouveau groupe de travail en « Groupe de travail sur la protection des données et les données policières et judiciaires en matière pénale » (CJ-PD/GT-PJ) [voir les documents CJ-PD-GC (2001) RAP 7 et CJ-PD (2001) RAP 39]. Le CDCJ et son Bureau ont été informés de ce changement de nom (voir paragraphe 35 du CDCJ-Bu (2002) 8) Le CJ-PD a insisté également pour que l'examen par le CJ-PD/GT-PJ de l'incidence des principes de la protection des données sur la coopération judiciaire en matière pénale accorde une importance particulière aux principes communs dont il faudra tenir compte pour répondre à des demandes d'entraide émanant de pays ne jouissant pas d'un niveau adéquat de protection de données.

3. Le mandat précité charge également le CJ-PD de « *préparer l'évaluation de la Recommandation n° R (87) 15 (police) devant être transmise au Comité des Ministres pour 2002, à sa demande et par l'intermédiaire du CDCJ* ».

4. Compte tenu de la similitude étroite entre les tâches du groupe de travail et le contenu de la Recommandation n° R (87)15, le CJ-PD a confié au CJ-PD/GT-PJ le soin de rédiger un projet de rapport consacré à la troisième évaluation de la Recommandation et devant lui être remis lors de sa 40ème réunion plénière de 2002 aux fins de révision et d'approbation. Le CJ-PD a demandé à son groupe de travail de prendre en compte les facteurs suivants lors de la rédaction du rapport : les deux évaluations précédentes, le séminaire régional « La protection des données dans le secteur de la police » organisé en 1999 par le Conseil de l'Europe dans le cadre de ses Activités pour le développement et la consolidation de la stabilité démocratique (ADACS) et de sa contribution au Pacte de stabilité pour l'Europe du Sud-Est, ainsi que les résultats du programme FALCONE lancé sur l'initiative des commissions italienne et portugaise de protection des données mais approuvé et parrainé par la Commission des Communautés européennes, de même que tout événement important éventuellement survenu depuis la dernière évaluation, notamment dans le cadre de la jurisprudence de la Cour européenne des Droits de l'Homme.

5. Conformément aux instructions susmentionnées, le CJ-PD/GT-PJ a préparé à la fois le présent projet de rapport sur l'incidence des principes de la protection des données dans le domaine judiciaire en matière pénale, y compris dans le cadre de la coopération judiciaire et le projet de rapport sur la troisième évaluation de la Recommandation n° (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Les deux projets de rapports seront soumis au CJ-PD lors de sa 40ème réunion plénière (7-9 octobre 2002) pour examen et approbation.

6. Le CJ-PD a examiné et révisé le Projet de rapport sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale au cours de sa 40ème réunion. Le CJ-PD a adopté ce rapport à l'unanimité, sauf le paragraphe 34 (sur le Principe de proportionnalité), sur lequel la délégation de Suède a exprimé une opinion divergente en ce qui concerne la destruction de données excessives qui, selon son avis, est en opposition avec les dispositions constitutionnelles de la Suède sur le droit d'accès aux documents publics. Le CJ-PD invite le CDCJ à approuver, sous réserve des amendements qu'il souhaiterait y apporter, le projet de rapport sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale, et à autoriser la publication de ce rapport sur le site web du Conseil de l'Europe.

7. Etant donné la composition multidisciplinaire[1] du Groupe de travail (CJ-PD/GT-PJ) qui a préparé le projet initial de ce rapport et la nature des questions abordées (données policières et judiciaires en matière pénale), le CJ-PD invite le CDCJ de faire parvenir pour information la version finale de ce rapport au Comité européen sur les problèmes criminels (CDPC) et, avec l'accord de ce dernier, à ses comités subordonnés compétents, notamment au Comité d'experts sur l'éthique de la police et les problèmes liés à l'exercice de la police (PC-PO) et au Comité d'experts sur le fonctionnement des conventions européennes dans le domaine pénal (PC-OC).

* * *

[1] Le CJ-PD a nommé les quatre experts suivants :

- M. Marc BUNTSCHU, Suisse (Chef suppléant du Secrétariat du Préposé fédéral à la protection des données)
- M. Giovanni BUTTARELLI, Italie (Secrétaire général de la Garante per la Protezione dei Dati Personali)
- M. Alexander PATIJN, Pays-Bas (Conseiller juridique au ministère de la Justice)
- Mme Kinga SZURDAY, Hongrie (Conseillère juridique principale au ministère de la Justice).

Conformément au mandat du CJ-PD, le Comité européen pour les problèmes criminels (CDPC) et ses comités subordonnés compétents peuvent également entrer dans la composition du CJ-PD/GT-PJ. C'est ainsi que trois autres experts ont été admis à siéger au CJ-PD/GT-PJ :

- M. Hughes BRULIN, Belgique (Conseiller juridique adjoint, Direction générale de la Législation pénale et des Droits de l'Homme du ministère de la Justice) a été nommé par le Comité européen pour les problèmes criminels (CDPC).
- Mme Elenor GROTH, Suède (Conseillère juridique au ministère de la Justice) a été nommée par le Comité d'experts sur l'éthique de la police et les problèmes liés à l'exercice de la police (PC-PO).
- M. Philippe BIJU-DUVAL, France (Adjoint au Chef, bureau du Droit communautaire et du Droit comparé, ministère de la Justice - service des Affaires européennes et internationales) a été nommé par le Comité d'experts sur le fonctionnement des conventions européennes dans le domaine pénal (PC-OC).

RAPPORT SUR L'INCIDENCE DES PRINCIPES DE LA PROTECTION DES DONNÉES SUR LES DONNÉES JUDICIAIRES EN MATIERE PÉNALE Y COMPRIS DANS LE CADRE DE LA COOPÉRATION JUDICIAIRE EN MATIERE PENALE

INTRODUCTION

8. Vingt ans après l'ouverture à la signature de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* [STE n° 108] du Conseil de l'Europe (ci-après désignée sous le terme « la Convention 108 »), certaines questions se posent encore à propos de l'incidence des principes de protection de ces données dans le contexte judiciaire, à savoir le traitement qui leur est réservé par les autorités judiciaires dans le cadre de procédures nationales ou internationales, ainsi que dans un contexte de coopération. L'Union européenne a amorcé une réflexion institutionnelle dans le cadre de la négociation de la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'UE* du 29 mai 2000 (JOCE, Série C 197, 12/07/2000). à la même époque, dans le cadre du « Projet sur la lutte contre le terrorisme et la protection des données à caractère personnel » (programme FALCONE) lancé sur l'initiative des commissions italienne et portugaise de protection des données et approuvé et subventionné par les Communautés européennes, des séminaires ont été consacrés à l'incidence de ces principes de protection sur les données en possession des autorités judiciaires. En outre, pendant la Conférence organisée par le Conseil de l'Europe, la Direction italienne anti-Mafia et l'université de Naples II sur la protection de la société contre la criminalité organisée, tenue du 8 au 10 septembre 2000 à Caserta (Italie), les procureurs européens ont mis l'accent sur la nécessité de constituer une banque de données centrale consacrée à la lutte contre la criminalité organisée. Ils ont fait cependant aussi remarquer le besoin d'imposer des restrictions à cet échange transfrontière de données afin de garantir les droits subjectifs, notamment en matière de protection des données à caractère personnel. Ils ont demandé au Conseil de l'Europe d'établir un comité d'experts chargé d'étudier ces questions et de formuler des recommandations appropriées. Le besoin d'élaborer des dispositions spécifiques dans ce domaine a d'ailleurs été réaffirmé lors des discussions précédant la mise en place d'Eurojust dans le cadre de l'Union européenne[2].

9. La question de l'incidence des principes de protection des données en possession des autorités judiciaires, y compris l'échange transfrontières d'informations dans le cadre d'une coopération judiciaire, est donc d'actualité et mérite d'être étudiée de plus près. C'est dans ce but que le Groupe de projet sur la protection des données (CJ-PD) a mis sur pied un groupe de travail approprié.

10. En vertu de l'article 3 de la Convention 108 : *« Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé »*. Le champ d'application de la Convention devrait donc en principe englober les données à caractère personnel relatives à des individus impliqués dans une procédure judiciaire et soumises à des traitements automatisés par le système judiciaire si les Parties à la Convention n'ont pas exclu ces catégories de fichiers automatisés à caractère personnel du champ d'application de la Convention, en conformité avec l'article 3, paragraphe 2, alinéa a, de la Convention 108. En outre, la

2 La Commission des Communautés européennes examine actuellement la manière dont il convient d'appréhender le problème de la protection des données dans le contexte de la coopération policière et judiciaire, afin de pouvoir faire une proposition.

Convention 108 peut aussi s'appliquer aux données judiciaires à caractère personnel ne faisant pas l'objet de traitements automatisés, pour peu que les Parties aient fait la déclaration mentionnée à l'article 3, paragraphe 2, alinéa c.

11. Cependant, le public n'a pris conscience que récemment de la possibilité d'appliquer les principes de protection des données aux données à caractère personnel en possession des autorités judiciaires. Ce constat s'explique concrètement par les règles spéciales de gestion des données observées pendant de nombreuses années en matière judiciaire et plus particulièrement par le contexte de l'adoption des Codes de procédure pénale respectifs des différents pays. La plupart de ces codes ayant été rédigés alors que l'informatique était encore inconnue ou limitée au secteur technique, l'application combinée des règles nationales de procédure et du principe de procès équitable conduisit naturellement les magistrats des pays européens à traiter manuellement les données judiciaires, à l'aide de classeurs et autres dossiers. En outre, la Convention 108 vise la collecte et le traitement d'informations fréquemment consultées, ce qui ne correspond pas au processus de traitement réservé habituellement aux informations utilisées dans le cadre d'une instruction ou d'un procès. Enfin et surtout, l'introduction du traitement automatisé des données à caractère personnel est relativement récente dans le domaine judiciaire.

12. Même si la Convention 108 était conçue pour s'appliquer au domaine judiciaire, il est de fait que les principes de la protection des données ne sont pas souvent appliqués dans ce domaine. Néanmoins, il existe certaines dispositions juridiques qui, bien qu'elles ne portent pas à proprement parler sur la protection des données, peuvent concourir à la réalisation du même but. Ainsi, par exemple, les Codes pénaux des différents pays, bien que n'ayant pas été rédigés dans l'esprit de la protection des données, recèlent de nombreuses règles - touchant notamment aux garanties accordées à l'accusé, aux modalités de recueil des preuves ou à la prise en compte des intérêts de toutes les parties dans un procès équitable - susceptibles d'avoir les mêmes effets que les principes de protection des données. En outre, les Codes pénaux ou les Codes de procédure pénale adoptés ou sérieusement révisés au cours des vingt dernières années incluent souvent des dispositions spécifiques à la protection des données en possession des autorités judiciaires.

13. Pendant près de quinze ans, le développement des nouvelles technologies de l'information dans la quasi-totalité des secteurs de la société s'est accompagné d'un renforcement parallèle de l'intérêt pour les organismes chargés de la lutte internationale contre la criminalité organisée. C'est pourquoi les autorités judiciaires des Etats européens ont établi des contacts et coopèrent au moyen des nouvelles technologies de l'information ; par exemple : consultation de bases de données sur les textes de loi et la jurisprudence, recours à des bibliothèques de modèles pour rédiger des projets d'arrêt et de décision, stockage de données spécifiques au cours de l'instruction, échange d'informations (voire de lettres rogatoires) au niveau international par courrier électronique, etc.

14. Les raisons évoquées ci-dessus soulignent la nécessité d'une étude approfondie de l'incidence des principes de protection des données sur l'activité judiciaire et plus spécialement sur le traitement des informations collectées à l'aide de méthodes intrusives (telles que l'interception des télécommunications) ou de nature à faciliter l'emploi de tests d'empreintes génétiques.

15. C'est pourquoi le Groupe de projet sur la Protection des données (CJ-PD) a préparé le présent rapport qui comprend deux parties principales : la première, intitulée « Incidence des principes de protection des données sur les données judiciaires dans le domaine pénal », analyse l'impact de ces principes sur les données traitées dans le domaine judiciaire et aborde plus particulièrement les

questions soulevées dans la pratique au niveau national ; la seconde, intitulée « Incidence des principes de protection des données sur l'entraide judiciaire en matière pénale », analyse l'impact de ces principes sur la coopération judiciaire internationale en matière pénale.

16. Il convient de rappeler que dans la mesure où le rapport fait référence à des garanties des droits et libertés fondamentales de tous, et notamment le droit au respect de la vie privée, tels qu'énoncés dans les articles 5, 6 et 8 de la Convention 108 et l'article 8 de la CEDH, des dérogations à ces droits, en conformité avec l'article 9 de la Convention 108, qui ont été élaborées sur la base de l'article 8 de la CEDH, sont possibles lorsqu'une telle dérogation est prévue par la loi et constitue une mesure nécessaire dans une société démocratique :

a. à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales ;
b. à la protection de la personne concernée et des droits et libertés d'autrui.

I. INCIDENCE DES PRINCIPES DE PROTECTION DES DONNEES SUR LES DONNEES JUDICIAIRES DANS LE DOMAINE PENAL

Remarques préliminaires

Approche adoptée par le Groupe de projet

17. Conformément à son mandat, le CJ-PD a été demandé d'examiner *« avant la fin de 2001 l'incidence des principes de protection des données sur, d'une part, la coopération judiciaire et, d'autre part, la coopération policière, en matière pénale […] »*. étant donné l'énoncé de sa mission, le CJ-PD a examiné l'incidence des dits principes dans le secteur judiciaire et préparé certains principes directeurs en la matière.

18. Dans la procédure pénale, des données à caractère personnel peuvent être traitées simultanément, y compris dans des documents identiques, par la police et par les autorités judiciaires. Les écoutes téléphoniques sont un bon exemple de la nature hybride de certaines données : en cas d'autorisation de l'écoute par un juge, les données sont recueillies par la police avant d'être transmises à nouveau à l'autorité judiciaire. Dans certains cas, par conséquent, les frontières entre les deux catégories s'estompent : certaines données policières sont transmises au secteur judiciaire, tandis qu'une partie des données judiciaires reste dans le secteur policier. Ceci peut rendre difficile la distinction entre données judiciaires et données policières et ne doit pas servir de prétexte pour éviter d'appliquer les principes de protection des données dans ces secteurs ou de déterminer qui est le maître du fichier ou quels sont les différents degrés de responsabilité impliqués par chaque opération de traitement. Néanmoins, il est clair que chaque niveau d'autorité doit respecter les règles qui sont les siennes.

19. Il convient de trouver des critères permettant de déterminer les règles spécifiques à appliquer. A cette fin, conformément à l'article 2.d de la Convention 108, le terme *maître du fichier* désigne *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées »*. Il est donc indispensable que la législation nationale de chaque pays détermine clairement si le maître

du fichier de données est l'autorité de police ou de justice. En outre, la finalité du traitement des données peut aussi servir de critère complémentaire.

20. Etant donné les considérations ci-dessus, la conclusion suivante est formulée :

La législation nationale de chaque pays doit établir clairement qui est le maître du fichier, au sens de l'article 2, paragraphe 2, alinéa d. de la Convention 108, en ce qui concerne les données judiciaires et les données policières. Il n'est pas nécessaire que le maître du fichier en ce sens soit la même autorité que l'autorité responsable des décisions relatives aux enquêtes pénales ou de la conduite de ces enquêtes. Une attention particulière doit être accordé à empêcher toute échappatoire en matière de responsabilités, en particulier dans les cas de collecte et d'utilisation par la police de données à caractère personnel sur la base d'une décision judiciaire autorisant le recours à des méthodes intrusives telles que l'interception de télécommunications.

21. Le CJ-PD a aussi précisé que les échanges de données par les autorités judiciaires dans le cadre d'une entraide judiciaire en matière pénale n'est qu'un aspect particulier du traitement de l'information et ne représente donc pas l'ensemble des activités impliquant le traitement de données à caractère personnel dans le domaine judiciaire. Les principes énoncés ci-dessous doivent par conséquent s'appliquer également aux autres activités de ce type.

22. Le CJ-PD a examiné la mise en œuvre des principes essentiels de protection des données dans le cadre de l'entraide judiciaire en matière pénale (voir la deuxième partie du présent rapport).

23. La portée de cet examen est limitée au traitement des données à caractère personnel dans le cadre de procédures judiciaires relatives à des affaires pénales, à l'exclusion des affaires civiles ou administratives. Quant à l'incidence des principes de protection des données sur le traitement des informations par les services de police, elle fait l'objet d'un rapport consacré à la troisième évaluation de la Recommandation n° (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

Protection des données et procédure pénale : un objectif commun ?

24. Il est possible que les principes de protection de données ne soient pas encore totalement appliqués (car peut-être non applicables) au domaine judiciaire. Il existe cependant des dispositions légales (voir la section précédente) poursuivant le même objectif, même si elles ne concernent pas spécialement la protection des données. C'est ainsi, par exemple, que les Codes pénaux des différents pays, bien que n'ayant pas été rédigés dans l'esprit de la protection des donnés, recèlent de nombreuses règles - touchant notamment aux garanties accordées à l'accusé, aux modalités de recueil des preuves ou à la prise en compte des intérêts de toutes les parties dans un procès équitable - susceptibles d'avoir les mêmes effets que les principes de protection des données.

Principes de protection des données

a) *Principe de licéité du traitement*

> *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont :*
> *a. obtenues et traitées loyalement et licitement ; »*

(Convention 108, article 5.a)

25. Ce principe exige que les autorités publiques ne puissent traiter des données à caractère personnel que si elles y ont été habilitées par la loi.

26. S'agissant du traitement des données de caractère personnel par les autorités judiciaires, il ne peut être tenu de fichier systématique des condamnations pénales hors du contrôle de l'autorité publique.

27. Compte tenu de l'incidence possible de la protection des données dans le contexte judiciaire, d'aucuns ont soulevé la question de savoir si ce principe, combiné au principe de transparence, exige des autorités judiciaires qu'elles disposent dans chaque cas d'une habilitation légale spécifique les autorisant à traiter des données en vue de poursuivre leurs buts légitimes.

28. Dans certains pays, la législation sur la protection des données ne s'applique pas aux procédures en cours, mais le Code de procédure pénale contient des dispositions spécifiques en matière de la protection des données. Plus généralement, les dispositions des Codes nationaux de procédure pénale contraignent les autorités judiciaires à accomplir leurs missions d'instruction et de jugement des affaires sans se référer explicitement au traitement des données ou à une liste exhaustive de finalités déterminées. à cet égard, il faut admettre que les dispositions traditionnelles des Codes de procédure pénale - qui n'ont pas été rédigées dans l'optique de la protection des données - peuvent répondre aux exigences de la Convention 108. C'est surtout le cas lorsqu'elles précisent les finalités des actions entreprises par les autorités judiciaires ou même lorsqu'elles évoquent ces activités dans les grandes lignes sans prévoir d'autorisation expresse de recours au traitement des données. Il serait donc souhaitable que les législateurs nationaux de l'ensemble des Parties à la Convention 108 examinent ce problème.

29. Concernant l'application du principe de protection des données tenant à la licéité du traitement des données judiciaires, la conclusion suivante est formulée :

Il n'est pas indispensable dans tous les cas d'invoquer des règles légales spécifiques autorisant les autorités judiciaires à traiter des données à caractère personnel pour répondre aux exigences du principe de licéité, lorsque le Code de procédure pénale contient déjà des règles similaires.

b) Principe de finalité

> *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont [...] enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités. »*
> (Convention 108, article 5.b)

30. Ce principe énonce que les données ne seront pas traitées ultérieurement à des fins incompatibles avec les finalités établies à l'origine.

31. Compte tenu de l'application possible de ce principe dans le contexte judiciaire, le problème consiste à opérer une distinction entre les fins compatibles et incompatibles (voir par exemple l'article 23.1.b de la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne* du 29 mai 2000). à titre d'exemple, un juge peut-il réutiliser dans le

cadre d'un procès civil (une procédure de divorce par exemple) des informations collectées lors d'un procès pénal portant sur des coups et blessures entre les mêmes époux ?

32. La réutilisation de données à des fins civiles est déjà discutable au plan de la compatibilité des finalités. Dans la plupart des affaires civiles, les parties fournissent elles-mêmes les données de leur plein gré. La réutilisation de données à des fins administratives semble encore plus problématique. La possibilité de réutiliser les données collectées dans le cadre d'une procédure pénale spécifique au cours d'une affaire administrative (douane, inspection du travail, fisc) devrait être considéré incompatible s'il n'y a pas de lien concret. Cela n'exclut pas que les exemptions et dérogations prévues à l'article 9 de la Convention 108 s'appliquent. Le Groupe de travail convient d'utiliser les mots *« directement liées »* utilisés à l'article 23.1.b de la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne* du 29 mai 2000.

33. Concernant l'application du principe de protection des données tenant à la finalité du traitement des données judiciaires, la conclusion suivante est formulée :

Si l'on considère que la réutilisation de données à caractère personnel collectées dans le cadre d'une procédure pénale est compatible avec ses finalités initiales, une attention particulière pourrait être prêté lorsque:
1) l'affaire pénale et l'affaire civile dans laquelle les données sont réutilisées sont directement liées ;
2) l'affaire pénale et l'affaire administrative pour lesquelles les données sont réutilisées sont directement liées.
Si la finalité pour laquelle les données sont réutilisées n'est pas compatible avec la finalité pour laquelle les données ont été collectées, il est possible d'invoquer les exemptions prévues par l'article 9 de la Convention 108.

c) *Principe de proportionnalité*

> *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont [...] adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées. »* (Convention 108, article 5.c)

34. Il est important d'évaluer, pour chaque catégorie de données, la nécessité de la collecte et du traitement ultérieur par rapport aux finalités du traitement. Le principe de proportionnalité, qui constitue le pendant du principe précédent, implique que les données faisant l'objet d'un traitement ne soient pas excessives au regard des finalités pour lesquelles elles sont enregistrées puis utilisées.

35. Il est déconseillé de transposer les principes de nécessité et de proportionnalité à la collecte des données par les autorités judiciaires sans clarifier auparavant le sens de ces termes. La jurisprudence de certaines commissions nationales de protection des données interprète en effet strictement ce mot en lui prêtant le même sens qu'à l'adjectif *indispensable* (par exemple, lorsqu'il est procédé à la collecte des données). Cependant, on peut fort bien estimer, au moment de la collecte d'informations par une autorité judiciaire, que ces données sont nécessaires, et constater ultérieurement, en fonction de l'évolution de l'enquête, qu'elles sont en fait dénuées de pertinence.

36. Ces principes de nécessité et de proportionnalité doivent donc s'apprécier globalement en gardant à l'esprit les différentes opérations de traitement effectuées au cours de la procédure (instruction et jugement d'une infraction pénale) dans le but essentiel d'établir la vérité dans le cadre d'un procès équitable. Ceci inclut la préservation des éventuelles données allant dans le sens de l'exonération de la responsabilité et des informations relatives au processus de collecte des données. Nombreux sont les cas où la détermination du caractère nécessaire ou proportionnel des données ne peut intervenir qu'à un stade ultérieur, postérieurement à la collecte. En revanche, à supposer que l'autorité judiciaire puisse établir dès le stade de la collecte que les données sont excessives, elle devra ordonner leur destruction. Dans le cas contraire, les données pourront être conservées pour une période restant à déterminer.[3]

37. La question de l'échange spontané d'informations entre les autorités judiciaires (d'un ou plusieurs pays) a été soulevée sous l'angle de l'application du principe de proportionnalité. Selon certains spécialistes, le même principe aurait déjà été implicitement admis par l'article 21 de la *Convention européenne d'entraide judiciaire en matière pénale* du 20 avril 1959 (STE n° 30). L'échange spontané d'informations entre services de police est explicitement mentionné à l'article 7 de la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union Européenne* du 29 mai 2000.

38. Concernant l'application du principe de protection des données tenant à la proportionnalité au traitement des données judiciaires, la conclusion suivante est formulée :

Le principe de proportionnalité devrait également s'appliquer au secteur judiciaire. Il convient cependant de l'apprécier avec la souplesse requise en gardant à l'esprit une vue d'ensemble de toutes les opérations de traitement effectuées pendant l'instruction pénale et le procès. L'exigence d'un procès équitable et la nécessité de préserver les éventuelles données allant dans le sens de l'exonération de la responsabilité réduisent la possibilité de prévoir les besoins en information des autorités menant ces activités.

d) Principe de la durée de conservation

> *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont [...] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. » (Convention 108, article 5.e)*

39. Selon ce principe, les données ne doivent pas être conservées plus longtemps que nécessaire. Cela ne signifie pas qu'elles doivent l'être le moins longtemps possible, la durée de la conservation dépendant en fait des finalités de la collecte de ces données.

40. Les autorités judiciaires peuvent traiter des données à caractère personnel dans le cadre d'enquêtes visant à réprimer les infractions pénales. Dans ce contexte, le traitement des données (y compris la

3 Le CJ-PD n'est pas arrivé à prendre une décision unanime à l'égard de ce paragraphe. La délégation de Suède a exprimé une opinion divergente, considérant que la destruction de données excessives est en opposition avec les règles constitutionnelles sur le droit d'accès aux documents publics. Le CJ-PD a procédé à un vote indicatif sur cette question : 14 délégations étaient en faveur de garder le texte tel quel et 10 délégations étaient en faveur de modifier le texte comme proposé par la délégation de Suède.

durée de leur conservation) est similaire à celui pratiqué par les services de police et peut donc se conformer aux règles communes énoncées dans le Principe 7.1 de la Recommandation n° R (87) 15. Cependant, dans la plupart des cas, la collecte et le traitement des données par les autorités judiciaires visent à servir de base à la procédure (procès) et à la décision (jugement) de justice. à cet égard, le groupe de travail considère que les dossiers judiciaires soient conservés plus longtemps car ils peuvent être nécessaires dans le cadre d'une procédure de révision. Lorsque la loi nationale fixe une limite temporelle à cette procédure de révision, le délai ainsi imparti détermine indirectement la durée de la conservation des données. Dans le cas contraire, une prolongation de la durée de conservation devrait être envisagée, dans l'objectif de l'éventuelle réparation d'une erreur judiciaire. Il convient sur ce point de tenir compte de la Recommandation du Comité des Ministres du Conseil de l'Europe n° R (84) 10 sur le casier judiciaire et la réhabilitation des condamnés et en particulier de son paragraphe 13 qui prévoit que *« la réhabilitation comporte l'interdiction de faire état sans motif impérieux, prévu par le droit national, des condamnations d'une personne réhabilitée »*.

41. Concernant l'application du principe de protection des données tenant à la durée de conservation des données judiciaires, la conclusion suivante est formulée :

Les données à caractère personnel servant de base à une décision de justice peuvent être conservées dans des dossiers judiciaires pour la durée nécessaire pour respecter les exigences de la procédure. Quand les données ne sont plus nécessaires pour respecter les exigences de la procédure pour laquelle elles ont été collectées, elles ne devraient être conservées qu'à des fins d'une procédure de révision ou à des fins de recherche historique, scientifique ou statistique. Leur conservation devrait être accompagnée de garanties appropriées et de mesures de sécurité afin d'éviter leur utilisation à d'autres fins.

e) *Principe de transparence*

> *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont obtenues et traitées loyalement »* (Convention 108, article 5.a)
>
> *« Toute personne doit pouvoir :*
> *a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ;*
> *b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ; »*
> (Convention 108, article 8, paragraphes a et b)

42. Le principe de transparence peut être mis en œuvre par la communication aux intéressés d'informations relatives aux modalités de la collecte et de l'utilisation des données les concernant, sauf dans les cas où les intéressés sont déjà informés de ces modalités ou bien si une telle procédure requiert des efforts disproportionnés. Le CJ-PD note que, dans la pratique, les tierces parties ne sont pas souvent informées correctement des données les concernant qui figurent dans un dossier judiciaire.

43. Ce principe s'impose également dans le contexte judiciaire, de sorte que les autorités judiciaires sont tenues d'informer les personnes dont les données figurent dans un dossier lorsque cette formalité

est nécessaire et ne requiert pas d'efforts disproportionnés, surtout en cas de recours à des méthodes intrusives telles que l'interception de télécommunications ou de courriers électroniques et de recherche et de saisie de données informatiques. Concernant les modalités de l'information, il convient de tenir compte des différents niveaux d'invasion de la vie privée des personnes concernées (suspects, tierces parties, etc.). Ces dernières peuvent être informées de l'initiative d'une autorité judiciaire par une notification émanant de l'organisme de contrôle compétent en matière de protection des données, ou même se voir communiquer des détails explicites sur les critères de collecte et de traitement des données. On peut également supposer qu'une fois l'enquête criminelle terminée, il devient impossible d'empêcher la communication d'informations aux personnes concernées pour des motifs tenant aux risques que pareille mesure ferait peser sur les résultats de ladite enquête. Bien que les règles relatives à l'organisation d'un procès équitable puissent aussi servir à protéger les droits de l'accusé en matière de protection de ses données, elles ne permettent pas toujours d'étendre cette protection aux données relatives à d'autres personnes (telles que les témoins ou les victimes) impliquées dans l'affaire.

44. Etant donné les considérations ci-dessus, le Groupe de travail a formulé la conclusion suivante :

En principe, les autorités judiciaires devraient informer les personnes dont les données sont incluses dans un fichier. Cette notification est particulièrement importante et nécessaire lorsque des mesures interférant avec la vie privée ont directement affecté la personne concernée.

f) Droit d'accès

> *« Toute personne doit pouvoir :*
> *[…]*
> *b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ; »*
> *(Convention 108, article 8.b)*

45. Le droit de toute personne d'obtenir l'accès aux données à caractère personnel le concernant est l'un des principes de protection des données les mieux connus. Concernant les données judiciaires, ce droit doit être reconnu à toute personne réclamant l'accès au dossier la concernant, qu'elle invoque les dispositions du Code de procédure pénale ou la législation relative à la protection des données.

46. Certains problèmes peuvent apparaître en cas de transfert de données à caractère personnel d'un pays à l'autre, dans la mesure où les mêmes données relèvent alors de différentes législations nationales ou internationales. Les échanges de données réalisés dans le cadre de systèmes d'information internationaux, tels que Schengen ou Europol, illustrent le risque d'apparition d'un « shopping » : les personnes désireuses d'accéder aux données s'adressent naturellement aux autorités des pays où la transparence de l'information est la plus grande. Lorsque les règles nationales exigent la divulgation des données, l'information échangée se retrouve soumise à des règles d'accès différentes, dans la mesure où le droit d'accès est celui prévu par la législation du pays où la demande est déposée. C'est pourquoi les autorités judiciaires doivent prendre conscience du fait que les données considérées comme confidentielles dans leur pays ne jouissent pas nécessairement du même régime dans les pays tiers. En principe, le critère matériel est le même : on ne doit pas porter atteinte aux finalités de la collecte des données. Toutefois, l'application de ce principe diffère d'un pays à l'autre. Ce problème est pris en compte, par exemple, à l'article 109, paragraphe 1, de l'Accord de Schengen qui indique que les autorités du pays communiquant

les données doivent avoir la possibilité de faire connaître leur point de vue sur la demande d'accès du sujet des données. Ce point de vue sera pris en compte mais ne sera pas nécessairement déterminant dans le pays où est exercé le droit d'accès. Une coopération internationale plus importante serait nécessaire si, en cas de doute, cette règle devenait une pratique plus générale.

47. Etant donné les considérations ci-dessus, le Groupe de travail a formulé la conclusion suivante :

Si la personne concernée demande l'accès aux données la concernant qui ont été transférées par les autorités judiciaires d'un pays tiers, les autorités du pays d'origine devraient avoir la possibilité de faire connaître leur point de vue avant d'accéder à la demande.

g) Principe de la qualité des données : droit de rectification et d'effacement

> *« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont [...] exactes et si nécessaire mises à jour. » (Convention 108, article 5.d)*
>
> *« Toute personne doit pouvoir :*
>
> *[…]*
>
> *c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention » (Convention 108, article 8.c)*

48. Ce principe impose que les données traitées soient exactes, mises à jour lorsque nécessaire, et rectifiées ou effacées lorsqu'elles sont incorrectes.

49. Cependant, la collecte de données dans le cadre de procédures pénales prend parfois la forme de rapports de police ou de dépositions de témoins pouvant contenir des inexactitudes, même en cas de respect des règles de procédure, voire des mensonges délibérés. Lesdits rapports ou dépositions font partie intégrante du dossier d'instruction et, en vertu des Codes nationaux de procédure pénale, il serait inconcevable de les rectifier.

50. Une telle information peut être considérée comme correcte (dans la mesure où la déposition reprise dans le rapport retranscrit fidèlement les déclarations), mais elle est incorrecte pour autant qu'elle vise des événements qui ne se sont pas produits ou des situations impossibles. Ces données ne doivent pas pour autant être supprimées pendant la durée de conservation du dossier judiciaire. En outre, les dossiers judiciaires peuvent également contenir des déclarations – émanant d'un magistrat, d'un représentant des services de police, d'un témoin ou d'une victime - dressant un portrait subjectif du suspect. Enfin, A supposer que des données collectées par une autorité judiciaire à un moment où elles étaient considérées comme nécessaires se révèlent ensuite dénuées de pertinence, elles devront néanmoins être conservées dans le dossier.

51. Des données à caractère personnel sont également considérées inexactes ou incorrectes dans les cas où les données sont correctes, mais présentent néanmoins une fausse image de l'individu si elles ne sont pas complétées par d'autres données pertinentes. Par exemple, si les données démontrent qu'un

individu a été suspecté d'avoir commis un crime, mais n'a pas été poursuivi parce qu'il avait établi un alibi valable, les données relatives à la suspicion doivent être considérées incorrectes si elles ne sont pas complétées par les faits qui ont empêché la poursuite de l'individu.

52. Il est difficile d'envisager la correction des données concernant un individu reconnu coupable qui sont pertinentes pour la condamnation. Cela ne concerne pas le fait que le dossier contienne des données relatives aux tierces personnes qui peuvent être sans rapport avec la condamnation. Leur correction peut néanmoins intéresser la personne concernée si, par exemple, les données sont utilisées dans une procédure administrative directement liée à la condamnation. D'autre part, il ne peut être porté atteinte à l'autorité de la chose jugée.

53. Etant donné les considérations ci-dessus, la conclusion suivante est formulée :

Il faut examiner si le droit pour un individu d'exiger la rectification et l'effacement des données le concernant, telles qu'elles sont contenues dans un dossier judiciaire peut être accordé conformément aux règles de procédure pénale appropriées. Si des données incorrectes qui figurent dans un dossier judiciaire sont contestées par la personne concernée, elle devrait avoir la possibilité d'y verser une déclaration rectificative, déclaration qui fera dès lors partie intégrante du dossier.

h) Principe du contrôle indépendant

> *« Article 1*
> *1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole.*
> *2. a. A cet effet, ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 de l'article 1 du présent Protocole.*
> *b. Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence.*
> *3. Les autorités de contrôle exercent leurs fonctions en toute indépendance.*
> *4. Les décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel. » (Protocole additionnel à la Convention 108, article 1, paragraphes 1 à 4)*

54. Des autorités nationales de contrôle de la protection des données ont été mises en place dans la quasi-totalité des pays d'Europe. Elles jouissent de compétences leur permettant d'assurer le respect et l'intégration au droit interne des principes énoncés dans la Convention 108 ainsi que des dispositions de la législation nationale en matière de la protection des données. Elles sont par conséquent également habilitées à surveiller, contrôler et vérifier l'application de ces principes dans différents secteurs. Néanmoins, dans certains pays, des autorités indépendantes de contrôle de la protection des données ont été mises en place pour contrôler les échanges d'information entre les autorités judiciaires et le traitement des données par ces mêmes autorités. Dans ces pays, on a considéré, d'une part, que les autorités de contrôle de la protection des données n'avaient en général aucune compétence juridictionnelle et que le principe de la séparation des pouvoirs législatif, exécutif et judiciaire ne

permettait pas le contrôle des activités du pouvoir judiciaire. D'autre part, comme les autorités judiciaires collectent et traitent elles-mêmes des données à caractère personnel, il est apparu que ceci pouvait également être soumis à un contrôle des autorités de contrôle de la protection des données. La Convention 108 et son protocole additionnel s'appliquent aux données à caractère personnel concernant les personnes impliquées dans une procédure judiciaire et qui sont traitées par les services judiciaires, sauf dans le cas où les Parties à ces instruments internationaux ont fait une déclaration excluant explicitement ces catégories de données de leur champ d'application, conformément à l'article 3.2.a de la Convention 108.

55. La pratique révèle une séparation empirique des compétences. C'est ainsi, notamment, que les autorités de contrôle de la protection des données sont habilitées à vérifier la licéité des systèmes d'information et soumettent des propositions ou des recommandations en ce sens aux autorités judiciaires, tout en restant compétentes en matière de contrôle du contenu de l'information. En tout état de cause, les deux institutions sont censées exercer leurs tâches de contrôle respectives dans un esprit de coopération équitable.

56. En outre, les législations nationales confèrent parfois aux autorités nationales de contrôle des pouvoirs judiciaires comparables à ceux des tribunaux en leur permettant de trancher définitivement un différend opposant deux parties. Les lois concernées érigent cependant les autorités judiciaires en instances d'appel, chargées d'examiner les pourvois intentés contre les décisions rendues en première instance par les autorités de contrôle (ce qui illustre bien les limites du pouvoir dont ces dernières disposent).

57. Si, en conformité avec la législation nationale, en vue du principe de la séparation des pouvoirs, les autorités générales de protection des données ne sont pas compétentes en ce qui concerne des données judiciaires des procédures en instance, les fonctions de contrôle peuvent être remplies par un juge.

58. Compte tenu de ces considérations ci-dessus, la conclusion suivante est formulée :

Les Etats sont libres de nommer différentes autorités publiques indépendantes chargées de contrôler et de surveiller la mise en œuvre des droits énoncés dans la Convention 108 et dans la législation nationale en matière de protection des données. Dans ce domaine, la répartition des compétences entre les autorités de contrôle et les autorités judiciaires restera du ressort du droit interne. Ces autorités devraient coopérer.
Dans le cas où la loi conférerait aux autorités de contrôle de la protection des données des pouvoirs judiciaires, il conviendra d'accorder une attention particulière au respect des droits des individus et plus spécialement au droit à un procès équitable.

i) Principe des mesures de sécurité

> *« Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés. »* (Convention 108, article 7).

59. Bien que le principe de transparence requiert que les détails d'un dossier soient rendus publics, cette transparence ne s'applique pas nécessairement aux données à caractère personnel contenues dans le dossier.

60. C'est dans le cadre de la discussion de ce principe que la question de la publication de verdicts sur l'Internet et sur CD-ROM a été soulevée : dans certains pays, le nom des personnes concernées y est indiqué alors que dans d'autres il est effacé, de manière à ce qu'il ne puisse pas être retrouvé à l'aide de logiciels de recherche. Les nouvelles possibilités techniques offertes par la société de l'information entraînent des risques potentiels du point de vue des droits et des libertés fondamentales des individus. Le groupe de travail considère que la compilation de jugements, même si elle permet d'identifier les personnes concernées à partir des détails des jugements, devrait être conçue de telle manière que les recherches nominatives effectuées sur l'Internet ou sur CD-ROM ne puissent pas aboutir. Des mesures législatives sont nécessaires si de ces précautions ne découlent pas d'une obligation générale de protection des données à caractère personnel.

61. Compte tenu de ces considérations, le Groupe de travail a formulé la conclusion suivante :

Les autorités judiciaires doivent tenir compte du risque accru d'invasion de la vie privée des personnes concernées que fait peser la publication de verdicts sur l'Internet ou leur mise à disposition sur CD-ROM. Les mesures nécessaires devraient être mises en œuvre pour empêcher la recherche illicite de données au moyen de logiciels de recherche.

* * *

II. INCIDENCE DES PRINCIPES DE LA PROTECTION DES DONNEES DANS LE DOMAINE DE L'ENTRAIDE JUDICIAIRE EN MATIERE PENALE

Dispositions de traités antérieurs d'entraide judiciaire ayant une certaine incidence sur la protection des données

62. Bien que la première clause visant explicitement la protection des données dans un traité d'entraide judiciaire figure dans la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne* du 29 mai 2000, plusieurs instruments internationaux antérieurs contiennent des dispositions ayant une certaine incidence sur la protection des données à caractère personnel.

63. Dans le cadre du Conseil de l'Europe, les questions relatives à l'entraide judiciaire sont réglées par la *Convention européenne d'entraide judiciaire en matière pénale* [STE n° 30] du 20 avril 1959 (ci-après désignée sous l'abréviation « Convention européenne d'entraide judiciaire »). à l'époque, le traitement automatisé des données à caractère personnel n'existait pas encore, ce qui explique l'absence dans cette convention de dispositions relatives à la protection des données. Toutefois, l'article 6 reflète la prise en compte par les rédacteurs d'une situation analogue : *« […] Les objets, ainsi que les originaux des dossiers et documents, qui auront été communiqués en exécution d'une commission rogatoire, seront renvoyés aussitôt que possible par la partie requérante à la partie requise, à moins que celle-ci n'y renonce. »*

64. La *Recommandation n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications* du 25 juin 1985 déclare expressément que : *« les autorités de la Partie requérante ne se servent pas des éléments de preuve contenus dans les enregistrements et transcriptions résultant de la surveillance à des fins autres que celles ayant motivé la commission rogatoire à l'égard de laquelle l'aide a été accordée »* (point 4.d de l'annexe à la Recommandation).

65. Une troisième disposition, antérieure aux clauses instituant explicitement une protection des données, figure dans les articles 8 et 9 du *Traité type d'entraide judiciaire en matière pénale* adopté par l'Assemblée générale des Nations Unies le 14 décembre 1990 (A/RES/45/117). L'article 8 traite des limites d'utilisation : l'Etat requérant ne peut utiliser ou transmettre des renseignements ou des preuves fournies par l'État requis pour des enquêtes ou procédures judiciaires autres que celles qui sont énoncées dans la demande. Quant à l'article 9, il traite de la protection de la confidentialité ce qui peut entraîner en conséquence la protection des données à caractère personnel. Le 20 janvier 1999, l'Assemblée générale des Nations Unies a adopté une Résolution intitulée *Entraide judiciaire et coopération internationale en matière pénale* (A/RES/53/112) dont les dispositions complètent le *Traité type d'entraide judiciaire en matière pénale*.

Dispositions de traités d'entraide judiciaire visant expressément la protection des données

66. La *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne* du 29 mai 2000 est la première à contenir des dispositions traitant explicitement de la protection des données. Son article 23 institue une protection générale :

> *« Article 23 – Protection des données à caractère personnel*
>
> *1. Les données à caractère personnel communiquées au titre de la présente convention peuvent être utilisées par l'Etat membre auquel elles ont été transmises :*
> *a) aux fins des procédures auxquelles la présente convention s'applique ;*
> *b) aux fins d'autres procédures judiciaires ou administratives directement liées aux procédures visées au point (a);*
> *c) pour prévenir un danger immédiat et sérieux pour la sécurité publique ;*
> *d) pour toute autre fin, uniquement après consentement préalable de l'Etat membre qui a transmis les données, sauf si l'Etat membre concerné a obtenu l'accord de la personne concernée.*
> *2. Le présent article s'applique aussi aux données à caractère personnel qui n'ont pas été communiquées mais obtenues d'une autre manière en application de la présente convention.*
> *3. Selon le cas d'espèce, l'Etat membre qui a transmis les données à caractère personnel peut demander à l'Etat membre auquel les données ont été transmises de l'informer de l'utilisation qui en a été faite.*
> *4. Lorsque des conditions concernant l'utilisation des données à caractère personnel ont été imposées conformément à l'article 7, paragraphe 2, à l'article 18, paragraphe 5, point b), à l'article 18, paragraphe 6, ou à l'article 20, paragraphe 4, ces conditions l'emportent sur les dispositions du présent article. En l'absence de telles conditions, les dispositions du présent article sont d'application.*
> *[…] »*

67. Des clauses spécifiques à la protection des données figurent : à l'article 7.2 concernant l'échange spontané d'informations (l'autorité qui fournit l'information pouvant soumettre à certaines conditions son utilisation par l'autorité destinataire) ; à l'article 13 concernant les équipes communes d'enquête (dont le paragraphe 10 énumère limitativement les fins auxquelles les informations obtenues par une équipe peuvent être utilisées) ; et aux articles 18, paragraphes 5 et 6, et 20 concernant l'interception des télécommunications (qui autorisent les Etats à définir les conditions d'utilisation des données interceptées).

68. Dans le cadre du Conseil de l'Europe, le *Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale* [STE n° 182] a été ouvert à la signature le 8 novembre 2001. L'article 26 de ce texte est explicitement consacré à la protection des données :

> *« Article 26 –Protection des données*
>
> *1. Les données à caractère personnel transmises d'une Partie à une autre en conséquence de l'exécution d'une demande faite au titre de la Convention ou de l'un de ses protocoles ne peuvent être utilisées par la Partie à laquelle elles ont été transmises :*
> *(a) qu'aux fins des procédures auxquelles s'applique la Convention ou de l'un de ses Protocoles ;*
> *(b) qu'aux fins d'autres procédures judiciaires ou administratives directement liées aux procédures visées au point (a),*
> *(c) qu'aux fins de prévenir un danger immédiat et sérieux pour la sécurité publique.*
> *2. De telles données peuvent toutefois être utilisées pour toute autre fin, après consentement préalable, soit de la Partie qui a transmis les données, soit de la personne concernée.*
> *3. Toute Partie peut refuser de transmettre des données obtenues en conséquence de l'exécution d'une demande faite au titre de la Convention ou l'un de ses protocoles, lorsque :*
> *- de telles données sont protégées au titre de sa loi nationale et*
> *- la Partie à laquelle les données devraient être transmises n'est pas liée par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg, le 28 janvier 1981, sauf si cette dernière Partie s'engage à accorder aux données la même protection qui leur est accordée par la première Partie.*
> *4. Toute Partie qui transmet des données obtenues en conséquence de l'exécution d'une demande faite au titre de la Convention ou l'un de ses Protocoles peut exiger de la Partie à laquelle les données sont transmises de l'informer de l'utilisation qui en a été faite.*
> *[…] »*

69. Le paragraphe 1 de cet article est similaire à l'article 23 de la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne* du 29 mai 2000. Le paragraphe 3 du même article règle la situation dans laquelle un Etat n'étant pas partie à la Convention 108 formule une demande d'entraide judiciaire.

70. La *Convention sur la cybercriminalité* [STE n° 185], ouverte à la signature le 23 novembre 2001, a été également rédigée dans le cadre du Conseil de l'Europe. Déjà signée par trente-trois Etats - dont quatre ne sont pas membres du Conseil : le Canada, le Japon, l'Afrique du Sud et les Etats-Unis

d'Amérique - elle a une portée mondiale, ce qui explique l'absence de toute disposition instituant explicitement une protection des données. Toutefois, son article 28 reproduit l'essentiel du *Traité type d'entraide judiciaire en matière pénale* des Nations Unies (mentionné plus haut) :

> *« Article 28 – Confidentialité et restriction d'utilisation*
>
> *1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.*
> *2. La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande :*
> *a. à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition, ou*
> *b. à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.*
> *3. Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.*
> *4. Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel ».*

71. Cet article autorise les Etats ayant ratifié la Convention 108 à limiter l'utilisation des données transférées à l'affaire spécifique pour laquelle elles ont été communiquées. Sur ce point, les paragraphes 275 à 278 du rapport explicatif sont parfaitement clairs :

> *« Confidentialité et restriction d'utilisation (article 28)*
>
> *275. Cette disposition prévoit expressément des restrictions à l'utilisation d'informations ou de matériel, de façon à permettre à la Partie requise, dans les cas où ces informations ou ce matériel sont de nature particulièrement délicate, de s'assurer que leur utilisation est limitée à celle en vue de laquelle l'entraide est accordée, ou qu'ils ne seront diffusés qu'aux services chargés de l'application de la loi de la Partie requérante. Ces restrictions constituent des garanties qui sont, entre autres, applicables aux fins de la protection des données.*
> *276. Comme l'article 27, l'article 28 ne s'applique que lorsqu'il n'existe pas de traité d'entraide ou d'arrangement reposant sur une législation uniforme ou réciproque en vigueur entre la partie requérante et la Partie requise. Lorsqu'un tel traité ou arrangement est en vigueur, ses dispositions touchant la confidentialité et les restrictions d'utilisation s'appliquent à la place des dispositions de cet article, à moins que les Parties audit traité ou arrangement en décident autrement. On évite ainsi tout chevauchement avec des traités d'entraide juridique bilatéraux et multilatéraux existants et des arrangements analogues, ce qui permet aux praticiens de continuer d'appliquer le régime habituel au lieu de*

chercher à appliquer deux instruments concurrents pouvant, éventuellement, se révéler contradictoires.
277. Le paragraphe 2 permet à la Partie requise, lorsqu'elle fait droit à une demande d'entraide, de fixer deux types de conditions. Premièrement, elle peut demander que les informations ou le matériel fournis restent confidentiels lorsque la demande ne pourrait être respectée en l'absence de cette condition, comme dans le cas de l'identité d'un informateur qui doit rester confidentielle. Il n'est pas approprié d'exiger une confidentialité absolue dans les affaires où la Partie requise est tenue de fournir l'aide demandée, car cela aboutirait souvent à gêner la Partie requérante dans la conduite de l'enquête ou de la procédure, par exemple en l'empêchant d'utiliser les éléments de preuve dans un procès public (y compris la divulgation obligatoire).
278. Deuxièmement, la Partie requise peut subordonner la communication d'informations ou de matériel à la condition qu'ils ne servent pas aux fins d'enquêtes ou de procédures autres que celles indiquées dans la requête. Cette condition ne peut s'appliquer que si son application est expressément demandée par la Partie requise; à défaut, la Partie requérante n'est pas tenue de respecter cette restriction à l'utilisation. Dans les cas où la Partie requise demande l'application de cette restriction, celle-ci garantit que les informations et le matériel ne pourront être utilisés qu'aux fins prévues dans la demande, excluant ainsi la possibilité qu'ils le soient à d'autres fins sans le consentement de la Partie requise. Les négociateurs ont prévu deux exceptions à la capacité de restreindre l'utilisation des informations, exceptions que le libellé du paragraphe fait ressortir de façon implicite. Premièrement, conformément aux principes juridiques fondamentaux de nombreux États, si le matériel transmis constitue des éléments de preuve disculpant un accusé, il doit être révélé à la défense ou à une autorité judiciaire. En outre, la plupart du matériel fourni dans le cadre des accords d'entraide est destiné à une utilisation lors de procès, normalement dans le cadre d'une procédure publique (y compris la divulgation obligatoire). Une fois qu'il a été divulgué, ce matériel tombe pour l'essentiel dans le domaine public. Dans ces situations, il n'est pas possible de garantir la confidentialité aux fins d'enquêtes ou de procédures pour lesquelles l'entraide a été demandée. »

72. La question s'est posée de savoir si l'on pouvait poser des conditions supplémentaires en arguant de ce qu'un transfert de données à caractère personnel vers un pays n'ayant pas ratifié la Convention 108 serait considéré par l'Etat requis comme contraire à ses intérêts essentiels. L'article 27, paragraphe 4, apporterait certains éléments de réponse en permettant à un Etat de refuser d'accéder à une demande d'entraide pouvant porter atteinte à ses intérêts essentiels. Les paragraphes 268 et 269 du rapport explicatif examinent ce point en détail :

« 268. Le paragraphe 4 prévoit la possibilité de refuser d'exécuter les demandes d'entraide présentées en application de cet article. L'entraide peut être refusée pour les motifs visés au paragraphe 4 de l'article 25 (c'est-à-dire les motifs prévus par le droit interne de la Partie requise), y compris l'atteinte à la souveraineté de l'État, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels, et lorsque la Partie requise considère l'infraction comme politique ou liée à une infraction politique. Au nom du principe supérieur consistant à accorder l'entraide la plus large possible (voir articles 23 et 25), les motifs de refus établis par une Partie requise doivent être limités et invoqués avec modération. Ils ne doivent pas prendre une ampleur telle qu'ils risqueraient d'aboutir à un refus d'entraide ou à l'octroi d'une entraide assortie de conditions trop lourdes au titre de vastes catégories de preuves ou d'informations.

269. Conformément à cette approche, il a été convenu que, outre les motifs de refus visés à l'article 28, le refus d'entraide au motif de la protection des données ne peut être invoqué que dans des cas exceptionnels. Une telle situation pourrait se présenter lorsque, après avoir pesé les intérêts importants impliqués dans un cas particulier (d'une part les intérêts publics, y compris la bonne administration de la justice et, d'autre part, des intérêts liés à la vie privée), il apparaît que la communication des données spécifiées, recherchées par la Partie requérante, soulèverait des problèmes d'une telle ampleur que la Partie requise pourrait les considérer comme relevant de motifs de refus fondés sur ses intérêts essentiels. Une application large, catégorique ou systématique des principes de protection des données pour refuser la coopération n'est, par conséquent, pas permise. Ainsi, le fait que les Parties concernées disposent de systèmes différents de protection du caractère privé des données (par exemple, la Partie requérante ne dispose pas de l'équivalent d'une autorité spécialisée en matière de protection des données) ou emploient des moyens différents pour protéger les données à caractère personnel (par exemple, la Partie requérante utilise des moyens autres que la procédure de suppression des données pour protéger le caractère privé ou l'exactitude des données à caractère personnel reçues par les autorités chargées de l'application de la loi), ne constitue pas, en soi, un motif de refus. Avant d'invoquer les « intérêts essentiels » comme motif pour refuser la coopération, la Partie requise devrait, à la place, essayer de fixer des conditions qui permettraient le transfert des données (voir Article 27, paragraphe 6 et paragraphe 271 de ce rapport). »

Application cohérente des traités d'entraide judiciaire

73. L'application des trois conventions (la *Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne* du 29 mai 2000, le *Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale* [STE n° 182] et la *Convention sur la cybercriminalité* [STE n° 185]) devrait être cohérente.

74. A cet égard, le problème tient aux pays qui ont conclu entre eux des traités d'entraide judiciaire sans devenir parties à la Convention 108 et qui sont donc réputés dépourvus d'un niveau de protection adéquat des données. Il convient alors de distinguer entre les trois cas suivants : a) existence d'un traité d'entraide judiciaire entre des pays ayant ratifié la Convention 108 ; b) existence d'un traité d'entraide judiciaire entre des pays ayant ratifié la Convention 108 et des pays ne l'ayant pas fait ou bien uniquement entre des pays n'ayant pas ratifié la Convention 108 ; c) absence d'un traité d'entraide judiciaire entre des pays n'ayant pas ratifié la Convention 108.

75. Le premier cas ne soulève aucune difficulté, le transfert des données à caractère personnel en vertu des traités d'entraide judiciaire concernant uniquement des pays censés être dotés d'un niveau de protection adéquat. Le troisième cas ne soulève, lui non plus, aucune difficulté puisque aucune norme internationale n'oblige le pays requis à accéder à la demande de transfert en vertu d'un traité d'entraide judiciaire ou de la Convention 108, de sorte que la notion de niveau de protection adéquat au sens du Deuxième Protocole additionnel à la Convention 108 s'applique sans la moindre restriction. Le deuxième cas est celui qui soulève les principales difficultés. Les Etats requis sont certes obligés de transférer les données en vertu des traités d'entraide judiciaire, mais les pays requérants n'ayant pas ratifié la Convention 108, ils sont considérés comme des pays tiers et donc admis à recevoir ces données uniquement s'ils disposent d'un « niveau de protection adéquat » : une notion qu'il est parfois malaisé de définir. Le rapport explicatif sur le *Protocole additionnel à la Convention pour la protection*

des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données [STE 181], et plus particulièrement ses commentaires relatifs au paragraphe 1 de l'article 2, fournit quelques éclaircissements sur la manière de déterminer la présence d'un niveau adéquat de protection des données dans un pays tiers. Deux approches sont possibles : une évaluation globale ou au cas par cas.

76. Le caractère adéquat du niveau de protection des données peut être établi sur la base d'une évaluation globale. Le paragraphe 28 du rapport explicatif sur le Protocole additionnel indique notamment que : *« Une appréciation du caractère adéquat peut toutefois être faite pour l'ensemble d'un Etat ou d'une organisation permettant ainsi tous les transferts de données vers cette destination. Dans ce cas, le niveau adéquat de protection est déterminé par les autorités compétentes de chaque Partie »*. En général, cependant, ce rapport donne l'impression de considérer cette approche globale comme l'exception plutôt que la règle.
Le caractère adéquat du niveau de protection des données peut être établi sur la base d'une évaluation au cas par cas. Le paragraphe 26 du rapport explicatif sur le Protocole additionnel indique notamment que : *« Le caractère adéquat du niveau de protection doit être évalué à la lumière de l'ensemble des circonstances relatives au transfert »*. Ce raisonnement est développé dans le paragraphe suivant du rapport : *« Le niveau de la protection devrait être évalué au cas par cas et pour chaque transfert ou catégorie de transfert effectué. Dans ce contexte, les circonstances relatives au transfert doivent être examinées et en particulier : la nature des données, les finalités et la durée des traitements pour lesquels les données sont transférées, le pays d'origine et le pays de destination finale, les règles de droit, générales et sectorielles applicables dans l'Etat ou l'organisation en question et les règles professionnelles et de sécurité qui y sont respectées. »*

77. Cependant, d'après l'article 2, paragraphe 2, du Protocole additionnel à la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, le transfert de ces données à des pays n'assurant pas un niveau de protection adéquat reste possible lorsque le droit interne le prévoit pour des intérêts spécifiques de la personne concernée ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou bien lorsque des garanties - pouvant notamment résulter de clauses contractuelles - sont fournies par le responsable du transfert.

78. Dans ce contexte, il est important de savoir en quoi pourraient consister les exceptions fondées sur la prise en compte par le droit interne d'*« intérêts légitimes, en particulier des intérêts publics importants »*. Le paragraphe 31 du rapport explicatif avance sur ce point la thèse suivante : *« Les Parties possèdent une marge d'appréciation pour déterminer les dérogations au principe de niveau adéquat. Les règles pertinentes de droit interne doivent néanmoins respecter le principe de droit inhérent à l'ordre juridique européen qui consiste à interpréter les clauses d'exception de manière restrictive afin que l'exception ne devienne pas la règle. Les normes de droit interne peuvent énoncer de telles exceptions pour un intérêt légitime, lorsque celui-ci prévaut. Cet intérêt peut être de protéger un intérêt public important, tel que défini dans le contexte de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme et de l'article 9, paragraphe 2, de la Convention STE n° 108 ; l'exercice ou la défense d'un droit en justice ; ou lorsqu'il s'agit de données extraites d'un registre public. Des exceptions peuvent également être prévues pour répondre à des intérêts spécifiques de la personne concernée, pour l'exécution d'un contrat conclu avec la personne concernée ou dans l'intérêt de celle-ci, pour la protection de ses intérêts vitaux ou lorsqu'elle a donné son consentement. Dans ce cas, avant de consentir, la personne concernée doit être informée de manière appropriée du transfert envisagé »*.

79. Les seules exceptions à la condition de niveau de protection adéquat admises par l'article 2, paragraphe 2, alinéa a, du protocole sont :
1) Les dispositions du droit interne :
Les exemples qui viennent à l'esprit concernent les dispositions du Code de procédure pénale, mais aussi la législation déterminant les compétences respectives des autorités policières et judiciaires ou les lois incorporant des conventions internationales à l'ordre juridique interne. Les possibilités offertes par le droit interne, notamment en matière de dérogation au principe de protection adéquate des données au nom d'intérêts publics importants, méritent un examen plus attentif. La prévention d'un danger important et imminent et la répression d'une infraction pénale grave peuvent tomber dans la catégorie des intérêts légitimes mentionnés dans le Protocole additionnel, sous réserve des garanties appropriées. Les activités de police doivent être, elles aussi, considérées comme menées dans le but de « protéger un intérêt public important » pour reprendre la terminologie de ce rapport. Il faudrait par conséquent assurer que le droit interne autorise les autorités de police à transférer des données dans la poursuite de ces tâches si les conditions pertinentes sont remplies.
2) Les dispositions du droit international (applicables en droit interne) :
Ces dispositions peuvent figurer dans des traités de coopération et d'aide militaires (par exemple le traité de l'OTAN), des accords de coopération policière, des arrangements prévoyant des échanges d'informations entre services de renseignement et, dernier point mais pas le moindre, des traités d'entraide judiciaire.

80. Une autre possibilité de déroger au principe de niveau adéquat de protection des données offert par destinataire vise les garanties fournies par la personne responsable du transfert dernier, en particulier celles résultant de clauses contractuelles. Les paragraphes 32 et 33 du rapport explicatif précisent sur ce point que : *« Chaque Partie peut également prévoir qu'un transfert de données à caractère personnel, vers un destinataire n'étant pas soumis à la juridiction d'une Partie et n'assurant pas un niveau de protection adéquat pour le transfert considéré, peut être effectué lorsque la personne responsable du transfert fournit des garanties suffisantes. Ces garanties doivent être jugées suffisantes par les autorités de contrôle compétentes, conformément au droit interne. De telles garanties peuvent notamment résulter de clauses contractuelles liant le responsable du traitement à l'origine du transfert et le destinataire n'étant pas soumis à la juridiction d'une Partie »*. Cependant, la nature contractuelle de ces clauses empêche leur application, dans le cadre d'affaires pénales, aux transferts de données visant une personne spécifique entre deux autorités de police. Des accords tels ceux élaborés dans le cadre d'Europol concernant la communication de données à des pays tiers et à des tierces personnes peuvent être utilisés. Il arrive que des conditions visant spécifiquement le traitement des données dans un but différent (la protection du caractère confidentiel des informations par exemple) aient des effets comparables aux mesures prises au nom de la protection des données. En pareil cas, un examen du transfert concerné pourrait permettre de conclure que les garanties fournies sont suffisantes. Une autre possibilité d'obtention de garanties suffisantes au sens du paragraphe 32 du rapport explicatif consisterait en un accord passé sous une forme quelconque entre le fournisseur et le destinataire ; le même rapport prévoit d'ailleurs des protocoles d'accord ou des accords spécifiques basés éventuellement sur des conditions générales.

81. La question de la série de conditions que doit remplir un pays pour être considéré comme offrant un niveau de protection adéquat ou bien de la détermination des cas où un transfert reste possible même en l'absence d'un tel niveau soulève des controverses. Le groupe de travail a néanmoins précisé que le transfert de données à caractère personnel à destination de pays tiers dépourvus d'un niveau de protection adéquat mais liés par un traité d'entraide judiciaire était possible dans certaines limites.

L'une des solutions envisageables serait d'examiner l'opportunité des transferts au cas par cas et d'invoquer éventuellement la clause de limitation d'utilisation figurant dans le traité concerné pour éviter que les données soient utilisées, sans autorisation expresse du pays requis, à des fins autres que celles indiquées dans la demande. Le *Deuxième protocole à la Convention européenne d'entraide judiciaire* autorise ce type d'arrangements, de même que la *Convention sur la cybercriminalité*. Pareille clause circonscrit l'utilisation des informations au cadre de l'affaire spécifique pour laquelle la demande d'entraide a été déposée. La certitude pour le pays requis de savoir que les données à caractère personnel qu'il s'apprête à livrer seront utilisées exclusivement aux fins pour lesquelles elles ont été communiquées l'incite à se montrer moins restrictif dans le transfert des données. Dans d'autres cas, le transfert pourrait être justifié par la défense d'intérêts publics importants en vertu de l'article 2 du protocole additionnel à la Convention 108. Enfin, peut se présenter le cas d'un pays requérant dépourvu d'un niveau de protection adéquat et d'une demande n'étant pas justifiée par un intérêt public majeur. Cependant, l'existence d'un traité d'entraide judiciaire rendant obligatoires les transferts pourrait être assimilée à un intérêt légitime prévalant.

82. Etant donné les considérations ci-dessus, la conclusion suivante est formulée :

L'examen de l'article 2 du Protocole additionnel révèle que diverses options s'offrent en matière de transfert de données à caractère personnel à des pays tiers *qui trouvent un* équilibre entre les principes de la protection des données et d'autres intérêts.
Les Parties qui transfèrent des données à caractère personnel en réponse à une demande d'entraide judiciaire d'un pays ne fournissant pas un niveau adéquat de protection devraient, à chaque fois que cela est possible, invoquer *une* clause de limitation d'utilisation figurant dans le traité concerné pour éviter que les données soient utilisées, sans autorisation expresse du pays requis si c'est en conformité avec le droit interne, à des fins autres que celles indiquées dans la demande. Toutefois, il ne sera pas nécessaire d'invoquer une telle clause dans le cas où la limitation d'utilisation découlerait directement du traité pertinent.