Principes directeurs sur la protection des données à caractère personnel à l'égard des cartes à puce (2004)

adoptés par le CDCJ lors de sa 79e plénière (11-14 mai 2004)

INTRODUCTION

Les comités du Conseil de l'Europe sur la protection des données souhaitaient attirer l'attention sur certains aspects de la protection des données à caractère personnel à l'égard de l'utilisation des cartes à puce. Le Groupe de projet sur la protection des données (CJ-PD) du Conseil de l'Europe a donc demandé à un consultant, M. Karel NEUWIRT (Président de l'autorité tchèque de protection des données) de rédiger un rapport sur la protection des données à l'égard de l'utilisation des cartes à puce. Ce rapport reconnaissant que toute étude des cartes à puce est liée aux avancées technologiques et doit donc être replacée dans son contexte historique, il avait été décidé de dresser une liste de principes directeurs spécifiques à prendre en compte en ce qui concerne l'utilisation des cartes à puce.

Après avoir examiné le rapport et les principes directeurs de M. Neuwirt, le CJ-PD a accepté de réviser et préciser certains de ces principes directeurs et a donc préparé le texte suivant.

Aux fins de ces principes directeurs, on entend par « carte à puce » un support mobile de données à caractère personnel doté de fonctions de traitement automatisé, qui est délivré à la personne concernée et traite des données à caractère personnel conformément aux objectifs et aux spécifications de l'émetteur par rapport à un système d'information y afférant. La carte peut être employée par exemple pour identifier la personne concernée, pour conclure des transactions qui ne peuvent pas être effectuées anonymement ou pour permettre l'accès à certains lieux et bases de données. Il convient de faire la distinction entre les cartes à puce et les cartes à piste magnétique ou à mémoire, qui ne peuvent pas être utilisées pour procéder à des opérations logiques et arithmétiques autonomes avec les données.

Les cartes à puce sont de plus en plus utilisées pour des applications variées. La nature et les capacités des cartes à puce soulèvent de nombreux problèmes de protection de données et il est indispensable d'apporter une réponse à ces nouveaux problèmes : Qui contrôle les données utilisées dans le système ? Qui est responsable de l'exactitude et de la sécurité des données lorsque le système est accessible à plusieurs entités tierces ? Comment limiter la multiplication des risques que les capacités des cartes à puce peuvent faire courir à la vie privée des citoyens ? Qui peut avoir accès aux données à caractère personnel du titulaire et dans quelles conditions ? etc.

Les systèmes d`information qui utilisent des cartes à puce impliquant le traitement de données à caractère personnel entrent dans le champ d`application de la Convention nº 108 du Conseil de l`Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [STE n° 108] (ci-après désignée par Convention 108). Cette Convention a été élaborée lorsqu'il est apparu clairement qu'il était nécessaire, afin de garantir la protection juridique efficace des données à caractère personnel, de développer plus spécifiquement et systématiquement la référence générale au respect de la vie privée énoncée à l'article 8 de la

Convention de sauvegarde des Droits de l`Homme et des Libertés fondamentales (ci-après désignée par CEDH).

Des droits et garanties supplémentaires sont énoncés dans diverses recommandations du Conseil de l`Europe, notamment :

a) la Recommandation nº R(2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d`assurance
b) la Recommandation nº R(99) 14 sur le service universel communautaire relatif aux nouveaux services de communication et d`information
c) la Recommandation nº R(99) 5 sur la protection de la vie privée sur Internet
d) la Recommandation nº R(97) 5 sur la protection des données médicales
e) la Recommandation nº R(95) 4 sur la protection des données à caractère personnel dans le domaine des services des télécommunications eu égard notamment aux services téléphoniques
f) la Recommandation nº R(90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes
g) la Recommandation nº R(89) 2 sur la protection des données à caractère personnel utilisées à des fins d`emploi
h) la Recommandation nº R(86) 1 sur la protection des données à caractère personnel utilisées à des fins de sécurité sociale
i) la Recommandation nº R(85) 20 sur la protection des données à caractère personnel utilisées à des fins de marketing direct

Un certain nombre d`activités et d'instruments du Conseil de l`Europe, en particulier les travaux de ses comités d'experts chargés de la protection des données à caractère personnel, sont indirectement associés aux questions soulevées par l`utilisation des cartes à puce. En particulier, étant donné que les cartes à puce peuvent être employées afin de stocker des données biométriques, il convient d'attirer l'attention sur les principes directeurs sur la protection des données à caractère personnel sous la forme de données biométriques, actuellement en cours de préparation par le T-PD. Les technologies modernes apportent un certain nombre d`améliorations dans la vie quotidienne des citoyens, au prix de certains risques en matière d`ingérence dans la vie privée. Le propos du présent document du Conseil de l'Europe n`est donc pas de dépeindre les avantages liés à l`utilisation des cartes à puce, mais de préciser la stratégie qui doit être adoptée afin d`améliorer la protection des données à caractère personnel dans le cadre de l'utilisation de cette technologie.

La collecte et le traitement des données à caractère personnel dans les systèmes utilisant des cartes à puce devraient respecter tous les principes de protection des données à caractère personnel énoncés dans la législation interne.

Les principes directeurs suivants ne prétendent pas apporter une solution exhaustive à tous les problèmes de protection de données liés à l`utilisation des cartes à puce. Ces dernières sont en effet toujours intégrées à un système d`information plus vaste dont la protection efficace globale dépend de nombreux facteurs et circonstances ainsi que du comportement des personnes entrant en contact avec lui. La technologie des cartes à puce évolue très rapidement. Ces principes

directeurs visent à définir des principes fondamentaux qui ne devraient pas changer sensiblement avec l`apparition d`innovations technologiques. Il serait malgré tout souhaitable de les compléter en fonction des progrès constants accomplis dans ce domaine.

Il doit être rappelé que, dans la mesure où ces principes directeurs contiennent des garanties pour les droits et libertés fondamentales de chacun, et en particulier le droit au respect de la vie privée tel qu'il est consacré dans les Articles 5, 6 et 8 de la Convention 108 et l'Article 8 de la CEDH, des dérogations à ces droits, conformément à l'Article 9 de la Convention 108, qui a été élaboré à la lumière de l'Article 8 de la CEDH, sont possibles si elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique dans le but de :

a. protéger la sécurité de l'Etat, la sécurité publique ou les intérêts monétaires de l'Etat, ou réprimer les infractions pénales ;

b. protéger la personne concernée ou les droits et libertés d'autrui.

S'agissant de ces dérogations, il conviendrait de souligner qu'elles devraient être interprétées de façon restrictive et qu'elles ne devraient être invoquées que dans des cas exceptionnels conformément à l'interprétation de l'alinéa 2 de l'Article 8 de la CEDH qui a été faite par la Cour européenne des droits de l'homme dans sa jurisprudence.

Les principes directeurs visent en premier lieu l'émetteur de la carte, qui est le premier responsable de la protection des données personnelles contenues sur la carte. Ils visent également tous les autres participants aux systèmes d`information - les concepteurs de projet, les directeurs et opérateurs sans oublier les personnes concernées elles-mêmes – qui devraient prendre en compte ces principes ; les principes énoncés devraient être appliqués de manière aussi uniforme que possible. C`est en effet le seul moyen de contribuer à l`amélioration de l`interopérabilité internationale et de la sécurité des applications de carte à puce.

PRINCIPES DIRECTEURS

1. La collecte et le traitement de données à caractère personnel au moyen de cartes à puce doivent être licites et loyaux. Seules les données à caractère personnel nécessaires à la réalisation des finalités pour lesquelles la carte est utilisée devraient être collectées et stockées sur la carte. Les systèmes employant des cartes à puce devraient être transparents[1] pour les personnes dont les données sont traitées.

2. Les données à caractère personnel collectées et stockées sur une carte à puce ne devraient l'être qu'à des fins légitimes, spécifiques et explicites. Elles ne devraient pas être utilisées ultérieurement de manière incompatible avec ces finalités.

[1] Ce droit à la transparence implique que la personne concernée soit informée des données conservées et de l'emploi qui en est fait.

3. Les obligations relatives à la protection des données à caractère personnel incombent à la personne qui détermine la finalité du système et les moyens utilisés pour atteindre cette finalité. Dans le cas d'une carte polyvalente, ceci implique que différents contrôleurs sont chacun responsables de leur partie de la carte.

4. Lorsqu'une carte à puce est utilisée à des finalités différentes, le traitement devrait être organisé de manière à ne pas utiliser les données pour des finalités pour lesquelles elles n'ont pas été collectées. Les données communes aux différentes finalités doivent être limitées au strict nécessaire.[2]

5. Les données à caractère personnel sensibles[3] devant être enregistrées sur la mémoire de la carte ne devraient être collectées que si cela est prévu par la loi ou avec le consentement explicite de la personne concernée[4]. Ces données ne peuvent être traitées que conformément aux garanties appropriées stipulées par la loi [5]. Si la collecte et le traitement de telles données sont basés sur le consentement explicite, la personne concernée devrait être en droit de retirer son consentement à tout moment. Le refus ou retrait du consentement ne devrait pas être sanctionné par des conséquences négatives pour la personne concernée[6.]

6. Les données enregistrées sur une carte devraient être protégées contre tout accès non autorisé ou accidentel, modification et/ou effacement. Les cartes devraient offrir un niveau de sécurité approprié compte tenu de l`état de la technologie, de la nature sensible ou non des données enregistrées, du nombre et du type d`applications prévues et de l'évaluation des risques potentiels[7]. Les modalités selon lesquelles les tiers peuvent avoir accès aux données enregistrées sur la carte doivent être établies au préalable pour chacune des finalités spécifiques pour lesquels la carte est utilisée.[8]

---

[2] Par exemple, dans le cas d'une carte à puce utilisée par une école à la fois à la caféteria et à la bibliothèque, seules les données communes à ces deux finalités, comme le nom de l'enfant et sa classe, devraient être partagées.

[3] Conformément à l'article 6 de la Convention 108, les données à caractère personnel sensibles comprennent « les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle […] [et] les données à caractère personnel concernant des condamnations pénales ». Sont également considérées sensibles les autres données définies comme telles par le droit interne.

[4] Toutefois, il peut y avoir des cas pour lesquels le droit interne ne permet pas que le consentement soit un fondement suffisant de la licéité d'une collecte ou d'un traitement.

[5] Ces garanties appropriées qui fournissent une protection supplémentaire pour les données peuvent être mises en place, par exemple, au moyen du cryptage des données, qui est l'outil le plus sophistiqué disponible actuellement. Il doit cependant être tenu compte des éventuels développements futurs de la technique.

[6] Si l'enregistrement de données à caractère personnel sensibles est nécessaire à la fourniture d'un service en faveur de la personne concernée et que celle-ci refuse de donner son consentement explicite ou le retire, alors le service ne lui sera bien entendu pas fourni.

[7] Si par exemple, les cartes sur lesquelles il n'y a qu'une puce à mémoire sont utilisées, en principe seules les données personnelles d'identification peuvent être enregistrées. D`autres critères peuvent également être pris en compte tels que la quantité de données, le nombre potentiel de lecteurs, les finalités du traitement, etc.

[8] Le risque de détournement des données conservées sur la carte augmente si elle incorpore des fonctions de paiement. Il est déconseillé de combiner la fonction de paiement intégrée dans la carte avec des applications au moyen desquelles les données sensibles à caractère personnel du titulaire de la carte sont enregistrées dans la carte.

7. Lorsque des données à caractère personnel sont collectées et stockées sur une carte à puce, la personne concernée devrait être informée des finalités du traitement, de l'identité du responsable du traitement, des catégories des données concernées et des destinataires ou catégories de destinataires des données stockées. D'autres informations[9] devraient être fournies aux personnes concernées lorsque cela est nécessaire pour garantir un traitement équitable des données à caractère personnel.

8. Lors de l'émission d'une carte, le porteur devrait être dûment informé de la manière d'utiliser sa carte ainsi que des mesures à prendre en cas de fraude ou de divulgation non autorisée[10].

9. Chaque fois que des données à caractère personnel sont échangées entre une carte à puce et le système, la personne concernée devrait en être alertée, à moins qu'elle ne le sache déjà. Ceci est particulièrement important dans le cas des cartes sans contact, c'est-à-dire lorsque la personne concernée n'insère ou ne présente pas elle-même la carte au système.

10. La personne concernée devrait avoir le droit d'accéder aux données à caractère personnel la concernant contenues dans la carte et devrait avoir le droit d'obtenir leur correction ou, si nécessaire, leur mise à jour[11].

11. Les données résultant de l`utilisation d'une carte à puce[12] devraient être effacées si elles ne sont plus nécessaires pour la finalité spécifique pour laquelle la carte à puce a été utilisée.

[9] Les informations à fournir à la personne concernée peuvent aussi inclure les spécifications techniques du système choisi.

[10] En particulier, l'attention du porteur de la carte devrait être attirée sur les conséquences pouvant résulter d'une mauvaise utilisation de la carte, d'une divulgation du moyen d'accéder à l'information (code par exemple), ou d'une divulgation des données et que sa responsabilité juridique pourrait être engagée dans certains cas.

[11] Un moyen de garantir l'accès est l'installation de lecteurs de carte.

[12] Un exemple de telles données est celles donnant des informations sur la date et le lieu auxquels la carte a été utilisée.