COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 6 novembre 2001 CJ-PD-GC (2001) 10 final

GROUPE DE COORDINATION
DU GROUPE DE PROJET SUR LA PROTECTION DES DONNÉES
(CJ-PD-GC)

RAPPORT SUR LA PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL CONCERNANT L'UTILISATION DE CARTES A PUCE

préparé par M. Neuwirt (République tchèque)

Mémorandum du Secrétariat
préparé par la
Direction des Affaires Juridiques

I. AVANT-PROPOS

La carte plastique à mémoire fait partie du quotidien depuis 1950, année où le Diners Club émit des cartes de paiement servant à l'identification de ses membres. La première carte de crédit en plastique fut ensuite émise par la Bank of America en 1960. Depuis cette époque, la carte a été largement utilisée dans divers domaines de l'activité humaine : dans le secteur bancaire, dans le monde des affaires, dans le domaine de la santé, etc. Plus tard, la carte fut équipée d'éléments de mémoire qui lui permirent de véhiculer de plus en plus de données. La capacité de ces éléments de mémoire augmenta avec les progrès de la technologie, de même que la quantité de données à caractère personnel des titulaires de cartes. Ces données permettent d'identifier le titulaire et de tracer son portrait dans le cadre du domaine d'émission de la carte (données sur la santé, données sur le paiement, données sur la consommation, etc.).

Il faut tout d'abord signaler que les cartes à puce sont seulement une partie d'un système plus vaste et complexe qui inclut des terminaux, des réseaux, des serveurs, des systèmes de personnalisation et des applications logicielles, ainsi qu'une gestion des clés de cryptage. Ce système ne peut être sûr que si chacune des parties l'est aussi.

Les cartes à puce sont seulement un maillon d'une longue chaîne.

- le phénomène «carte» comme complément du phénomène «net»

La carte à puce est considérée comme un outil spécifique d'amélioration de la qualité générale de la société de l'information actuelle. Le phénomène de la carte à puce s'oppose donc aux réseaux et plus particulièrement à l'Internet dont l'architecture ouverte explique le succès mais aussi les failles au niveau de la sécurité. Les cartes représentent des outils individualisés et perfectionnés par rapport au réseau partagé (mais unique).

Alors que les cartes offrent des fonctions multiples, telles que la signature électronique ou le cryptage et le stockage des informations sélectionnées, les réseaux permettent un accès universel à l'information et au savoir. Seule une utilisation combinée des deux outils permet aux utilisateurs/citoyens de tirer un profit maximal des progrès technologiques. C'est pourquoi, les synergies entre les cartes et les réseaux, au sein d'une société avancée de l'information, méritent d'être analysées, afin de formuler des recommandations portant sur la mise au point de solutions appropriées.

En ce sens, la plate-forme double carte + réseau ouvre la voie à des applications souhaitables et mérite d'être prise en considération comme technologie complémentaire, tant en ce qui concerne ses avantages que ses risques.

- la carte en tant qu'outil renforçant la sécurité - génération/conservation de clés

L'utilisation adéquate et fiable des technologies de traitement et de transmission des données est une condition essentielle au fonctionnement harmonieux de la société de l'information moderne.

Les cartes à puce incluent des fonctions de sécurité reposant sur des procédés très spécifiques et individualisés : elles servent à collecter des données à caractère personnel sur le titulaire, mais comportent aussi, en supplément, un utilitaire de traitement permettant au titulaire et au système de contrôler l'accès à leur contenu.

Alors que dans le passé, nombre de projets essayaient de bâtir leur infrastructure de communication sur des cartes ou des réseaux, la plupart des spécialistes s'accordent désormais à penser que seule une utilisation combinée des fonctionnalités respectives des cartes et réseaux permettra de répondre

à certains besoins en matière de sécurité, de protection de la vie privée et d'accès universel aux données à caractère personnel.

L'une des caractéristiques essentielles de la technologie des cartes à puce tient à sa capacité à générer des clés cryptographiques sur le support lui-même. En plus de cette capacité, la carte offre des fonctions de signature électronique et de cryptage et se trouve déjà à un état de normalisation avancé. Elle constitue par conséquent un outil sans égal. Il convient de noter que le GSM[1] est souvent considéré comme une solution concurrente potentielle reposant sur l'utilisation d'un téléphone portable au lieu d'une carte à puce. Mais le GSM est en fait basé lui-même sur une carte à puce insérée dans le téléphone et appelée SIM[2], de sorte que le téléphone portable n'est rien d'autre en fait qu'une interface entre une carte intelligente et l'utilisateur. De ce point de vue, il est donc superflu de dissocier les règles et recommandations applicables aux utilisateurs de cartes et de GSM.

L'utilisation de cartes à puce cryptographiques implique l'établissement d'infrastructures publiques de gestion de clés, réservant l'accès des données pertinentes aux titulaires d'une autorisation permanente. Il convient donc de construire et d'exploiter des infrastructures harmonisées au niveau international. La nécessité d'une telle interopérabilité universelle est d'ailleurs évidente.

- la carte autorise une gestion hors ligne efficace des transactions

Outre la sécurité, les cartes offrent un avantage commercial non négligeable en ce sens qu'elles permettent de gérer des transactions hors ligne sécurisées. Cette capacité repose essentiellement sur l'autorisation de l'utilisateur - une procédure permettant au titulaire de prouver sa relation à la carte - et sur l'authentification réciproque de la carte et du système d'information auquel elle est reliée.

Le fonctionnement hors ligne est important pour deux raisons essentielles :

- Premièrement, il rend possible la mise en place de solutions permettant d'économiser des frais de communication en ligne (et en temps réel) tout en permettant de résoudre des situations d'urgence lorsque la connexion en ligne est indisponible pour un motif quelconque.

- Deuxièmement, les procédures hors ligne introduisent une nouvelle catégorie de risques qu'il convient de prendre en compte. Ces dangers découlent du calcul hors ligne qui, même s'il est sécurisé, n'est pas soumis au contrôle de puissants serveurs spécialisés (offrant la sécurité supplémentaire de pouvoir authentifier la station distante).

Les cartes à puce peuvent cependant offrir des solutions suffisamment fiables à ces problèmes.

Les cartes électroniques ont joué un rôle encore plus important dans la création d'une société de l'information. C'est pourquoi, l'Union européenne, lors de la conférence tenue à Lisbonne en avril 2000, décida d'aborder la question des cartes à puce dans le cadre de l'initiative «eEurope 2002 : une société de l'information pour tous». Le programme charte des cartes à puce, qui contient 12 sous-programmes, relatifs aux divers problèmes liés à l'application et à l'utilisation pratique de cette technologie, a été ratifié.

L'expansion attendue de l'application des cartes à puce va être accompagnée d'une augmentation du traitement des données à caractère personnel. Avec une quantité de plus en plus importante de données à caractère personnel stockées dans la mémoire de la carte, les risques de détournement de l'utilisation de ces données et d'atteinte à la vie privée du titulaire de la carte augmentent également. L'objectif de ce rapport est d'attirer l'attention sur ces risques et d'énoncer des principes garantissant leur minimisation.

---

[1] GSM : acronyme de l'anglais «Global System for Mobile communications» (réseau de téléphonie mobile)
[2] SIM : acronyme de l'anglais «Subscriber Identity Module» (module d'identification d'abonné)

II. ASPECTS TECHNIQUES

DEFINITIONS

Il existe plusieurs catégories de cartes à puce qui se distinguent par leurs caractéristiques. Aux fins du présent rapport, nous établirons une distinction fondamentale basée sur les caractéristiques liées à la *fonction* et à *l'accès*.

Au niveau du fonctionnement, nous distinguons deux types de cartes :

Une ***carte à puce*** est une carte dont la forme est définie[3], qui contient un ou plusieurs circuits intégrés (CI), est capable de stocker des données et permet l'accès à des systèmes d'information. Elle est pourvue d'un dispositif de sécurité et est dotée de sa propre identité. Elle est la possession d'une seule personne et permet d'effectuer au quotidien une ou plusieurs opérations. Un microprocesseur y est intégré, ce qui lui permet d'effectuer des opérations intelligentes. Elle est dotée en propre d'un système d'exploitation et de mémoires.[4]

Une ***carte à mémoire*** est une carte qui contient un circuit mémoire intégré. Elle se caractérise par un faible niveau de protection et une technologie sûre.[5] Les cartes à mémoire ont été utilisées pour certaines applications du secteur sanitaire et sociale et dans les premiers systèmes de téléphone à pré-paiement. Elles ne sont plus très répandues.

Les cartes se distinguent aussi en fonction du type d'accès :

Carte à puce à contact – il s'agit d'une carte à puce pourvue de contacts électroniques servant d'interface et permettant de communiquer avec des systèmes externes. Les données ne peuvent être lues de la mémoire que si la carte est insérée directement dans un lecteur de cartes.

Carte à puce sans contact – carte à puce utilisant es ondes radio basse fréquence comme source d'énergie pour communiquer avec des lecteurs de carte à puce.[6] La communication avec le monde extérieur se fait par une antenne enroulée dans la carte.

Certaines applications à fonctions multiples utilisent des cartes dites duelles, dans lesquelles les deux techniques d'accès aux données sont réunies.

Un ***détenteur de carte*** est une personne physique dont les données à caractère personnel sont stockées sur la carte en sa possession.

BREF HISTORIQUE DES CARTES

Les cartes à puce sont une invention européenne. On s'accorde généralement à faire débuter leur histoire en mars 1974, date du dépôt d'un brevet par le technicien français Roland Moréno. Ce dépôt représentait l'aboutissement d'efforts en matière de développement international. Une normalisation rapide rendit ensuite possibles l'application et l'utilisation industrielles de cette technologie.

Sur le plan des innovations, plusieurs étapes méritent d'être mentionnées :

---

[3] La taille de la carte et l'emplacement du circuit intégré sont généralement définis par une norme ISO (p.ex. ISO 7816-2).

[4] Le système d'exploitation d'une carte à puce est généralement installé dans la carte par le fabricant et ne peut être remplacé.

[5] Avec circuit EEPROM (Electrically Erasable Programmable Read-only Memory).

[6] La plupart des cartes à puce sans contact peuvent être lues à une distance d'environ quinze centimètres. La lecture peut se faire même si la carte est dans un portefeuille ou un porte-monnaie.

- cartes à mémoire - porteuses de données

L'année suivante (en 1975), une carte GAB (Guichet Automatique Bancaire) à mémoire fut testée avec succès et remplaça les cartes magnétiques. Ce simple changement de porteuse n'entraîna pas d'amélioration de la sécurité des données ; celles-ci demeuraient en effet accessibles «au public». Il permit cependant de vérifier et de confirmer l'utilisation pratique de la nouvelle technologie. Cette conclusion incita le secteur bancaire à débloquer les fonds nécessaires à un changement technologique qui dure maintenant depuis 25 ans ; il correspond à une politique rationnelle, tant sur le plan des coûts élevés que de l'intégration compliquée d'applications nouvelles et ingénieuses.

- cartes basées sur un microprocesseur

Entre 1974 et 1984, un certain nombre de brevets furent déposés qui permirent de lancer la production industrielle de cartes à puce standardisées. En même temps que Bull en France (1985), ORGA (Allemagne) présenta la première carte à puce multifonction lors de l'exposition commerciale CeBIT. Cette version gérait en plus l'autorisation du titulaire de la carte par celle-ci, ainsi que l'authentification (vérification réciproque) de la carte par le système hôte.

Seul l'avènement du micro-ordinateur permit de lancer la construction de systèmes fondamentalement sûrs.

- extension vers des systèmes d'exploitation perfectionnés

Les progrès dans l'architecture de la carte à puce furent suivis, au bout d'un certain temps, d'une amélioration de son logiciel et plus particulièrement de son système d'exploitation. La conception originale, dérivée des moniteurs logiciels associés aux micro-ordinateurs à une seule puce, fut progressivement remplacée par des systèmes d'exploitation professionnels garantissant une gestion sécurisée des cartes multifonctions dans le cadre de la norme ISO 7816.

Alors que les cartes téléphoniques à pré-paiement dotées d'une mémoire étaient déjà d'un usage répandu en 1990, leur principale application actuelle (GSM) n'est à la portée de l'industrie de cartes à puce que depuis un an.

- solution multifonction et multiapplication

Le décollage rapide du GSM vers 1995 suscita également un regain d'intérêt pour des applications visant d'autres segments du marché - plus particulièrement dans le domaine de la banque, des systèmes de fidélisation de la clientèle et des procédures d'identification fiables - et proposant un accès sécurisé à l'Internet, ainsi qu'aux systèmes de commerce, de santé et d'administration («e-government») en ligne…

Le coût des investissements associés à l'application générale de la technologie des cartes à puce est néanmoins trop élevé (selon certaines estimations, il atteindrait entre 3 et 7% du chiffre d'affaires annuel dans les secteurs des soins de santé et de l'assurance maladie) ; c'est pourquoi, certaines demandes légitimes se font jour en faveur de cartes polyvalentes. Du point de vue technique, un tel regroupement des applications serait parfaitement envisageable. Concernant cependant l'identification uniforme, l'agrégation et l'exploration en profondeur des données sur la carte, ainsi que la génération de profils d'utilisateur, les problèmes qui émergent sont difficiles à maîtriser.

Les cartes généralement utilisées de nos jours comportent une ou plusieurs fonctions. Dans la pratique, cela signifie qu'elles sont émises par un seul organisme chargé de gérer la base de données dont elles constituent l'extension naturelle. L'organisme d'émission gère ensuite les données sur une base contractuelle et rend leur utilisation possible dans le cadre de ses propres applications ou d'applications qu'il exploite pour des tiers.

Concernant l'utilisation future, à savoir après 2001, on prévoit que des cartes multiapplications, très semblables sur le plan fonctionnel à des ordinateurs personnels, seront distribuées au grand public.

Il deviendra alors possible d'acheter une carte vide dans laquelle chaque titulaire insérera le jeu d'applications correspondant à son choix.

- *fonctions de sécurité améliorées*

Les cartes à puce font partie d'une famille de technologies assurant la confidentialité des communications et l'authentification et la vérification de l'identité de l'utilisateur. Ces technologies sont appelées « Privacy Enhancing Technology (PET) » (technologies renforçant la protection de la vie privée). Elles incluent des logiciels de cryptage, des mécanismes permettant l'utilisation anonyme du matériel, des outils d'identification biométrique pour la sécurité et la confidentialité des transactions et d'autres techniques préservant l'anonymat des communications.[7]

Depuis environ 1993, de nombreuses mesures sont à l'étude en vue de prévenir les pratiques frauduleuses apparues avec l'introduction massive des applications de carte à puce (surtout celle des cartes à mémoire non protégées). Ces mesures, prises initialement par les seuls producteurs et opérateurs, culminèrent en France avec la création du SEFTI[8] et de la BCRCI[9] ; des institutions similaires ont d'ailleurs été aussi établies dans d'autres pays.

Afin d'accroître la sécurité des cartes à puce, deux principes fondamentaux ont été progressivement appliqués depuis 1997-1998.

Une carte est considérée comme un produit spécifique dont les propriétés sont progressivement améliorées :

- introduction de systèmes d'exploitation multifonctions capables de contrôler les droits d'accès au microcircuit intégré (la «puce»),
- ajout d'éléments matériels dédiés, tels que des générateurs de nombres aléatoires, des cryptoprocesseurs, des générateurs de clés cryptographiques ou des détecteurs d'état anormal de la puce
- insertion de mécanismes d'autodestruction chargés de détruire la carte en cas de détection d'une tentative d'emploi abusif.

- *développement de l'infrastructure*

Le simple résumé de l'évolution de la carte fait nettement ressortir sa nature spécifique, telle qu'elle résulte de sa conception globale hors du commun.

Parmi les principaux autres composants, signalons les terminaux sécurisés (surtout les terminaux multiapplications), les enregistrements de transmission destinés à la collecte des données transactionnelles et le logiciel équipant les serveurs de collecte des données et les bases de données.

Les normes contraignantes et les règles éthiques exercent une influence considérable ; sans leur acceptation, il serait impossible d'harmoniser ou même d'exploiter des systèmes de masse basés sur les cartes à puce.

Dans le cadre de ses efforts visant à examiner et à résoudre ces problèmes au niveau international, la Commission européenne lança en 2000 une initiative dite «Charte des cartes à puce eEurope», dans le cadre du programme relatif aux Technologies de la Société de l'Information (TSI)[10].

Les cartes à puce sont détenues par des citoyens qui les considèrent comme un bien privé, personnel et sûr, placé sous leur contrôle. Elles sont perçues comme des jetons fiables hébergeant des données

[7] Voir par exemple Borking J.J.: On PET and other privacy supporting technologies (www.privacyservice.org)
[8] SEFTI : Service d'Enquête sur les Fraudes aux Technologies de l'Information
[9] BCRCI : Brigade Centrale de la Répression de la Criminalité Informatique
[10] voir le site http://www.eurosmart.com

à caractère personnel. Lorsqu'il utilise sa carte à puce, le citoyen peut être assuré d'un accès et d'un fonctionnement sécurisés dans le cadre d'une interface (présentation) homogène et conviviale.

APERÇU DES TECHNOLOGIES EXISTANTES

Les applications de la vie réelle reposent généralement sur plusieurs technologies utilisées en parallèle.

Si l'on considère l'évolution de la technologie des cartes, depuis le simple rectangle de plastique pur jusqu'à la carte à puce (abritant un circuit, un système d'exploitation et un logiciel d'application intégrés), on peut élaborer la classification élémentaire suivante :

- *Classification des cartes en tant que porteuses de données*

  Toutes les cartes en plastique permettent d'imprimer des données visibles, telles que le nom ou la photo du titulaire, sur leur surface. Certaines de ces données peuvent donc être lues par des machines, par exemple à l'aide d'un procédé ROC[11]. Certaines données sont gravées en relief sur le plastique afin de permettre l'impression de bordereaux correspondant aux transactions effectuées à l'aide de la carte. Il est même possible de placer des données visibles mais incompréhensibles (par exemple un code à barres) sur la surface. Toutes ces précautions dépendent de la technologie de carte utilisée.

  A l'opposé, certaines données destinées à un traitement automatisé sont placées sur la puce, écrites sur la bande magnétique ou gravées au laser dans le champ optique de la carte. Dans ce cas, les données peuvent éventuellement être enregistrées sous une forme cryptée. À l'exception de celles placées dans le microcircuit intégré, toutes les données sont encore publiquement accessibles et doivent être traitées en conséquence. Même si ce fait échappe parfois au titulaire, les données peuvent être facilement récupérées - sur la bande magnétique, le champ optique ou la mémoire non protégée de la carte - à l'aide d'un simple lecteur approprié.

  On a eu recours à des mémoires non réinscriptibles pour protéger les cartes contre une émission frauduleuse. De nombreuses précautions, élaborées à l'origine pour l'imprimerie (c'est le cas notamment des filigranes), visent à empêcher la copie du corps en plastique.

- *Traitement amélioré*

  Le microprocesseur, avec sa puissance de traitement, permet d'assurer les principales défenses du système :

  - Gestion de l'environnement du micro-processeur (physique et électrique) autour de la puce de la carte et facilité d'autodestruction éventuelle.
  - Définition et gestion des droits d'accès aux structures de données situées sur la puce.
  - Génération de nombres aléatoires pour contrôler la puce.
  - Calcul de la signature électronique à l'aide d'une clé privée et vérification des clés reçues.
  - Cryptage et décryptage des flux de données internes.
  - Recours à des cryptocartes prenant en charge la génération des clés et simplifiant l'installation de la PKI[12], aucune dissémination des clés privées n'étant requise.

[11] ROC : Reconnaissance Optique des Caractères
[12] PKI : acronyme de l'anglais «Public Key Infrastructure» (infrastructure des clés publiques)

- *Caractéristiques de la communication des cartes électroniques avec l'environnement extérieur.*

  La carte à puce abrite un circuit intégré doté d'un système d'exploitation et d'un logiciel d'application ; il s'agit donc en fait d'un petit ordinateur.

  La méthode habituelle de communication entre la carte et le monde extérieur repose sur des contacts fixés mécaniquement sur la carte à l'intérieur du lecteur de carte.

  Dans certains cas, les utilisateurs ont du mal à insérer leur carte dans la fente étroite ou bien se retrouvent devant des fentes ouvertes et par conséquent exposées à des conditions extrêmes réduisant sensiblement la fiabilité du lecteur. D'où le succès des cartes sans contact conformes à la norme ISO 14443.

  Les cartes sans contact ou hybrides (avec et sans contact) peuvent être détectées à distance, ce qui semble constituer un avantage dans la pratique mais introduit le risque d'une surveillance éloignée ou d'un traitement involontaire des transactions.

  Il convient donc de ne pas utiliser de carte sans contact lorsque des informations autres que les données personnelles du titulaire sont passées au scanner.

- *Authentification des titulaires de carte*

  Certaines technologies (mot de passe, PIN) permettent de sécuriser l'accès aux systèmes d'information distribués. Ces technologies nécessitent un minimum de mémoire et un algorithme de traitement, mais elles peuvent être jugées insuffisantes dans de nombreuses circonstances. Elles ne sont pas très sûres et peuvent être assez facilement détournées de leur usage.

  L'identification du titulaire de la carte par des signes biométriques - empreinte digitale, géométrie de la main, lecture d'empreintes rétiniennes ou iridiennes - est une forme d'identification plus sûre. La biométrie repose sur une procédure automatisée d'identification personnelle à partir de caractéristiques physiques ou comportementales. Pour que ces systèmes fonctionnent, le détenteur de la carte doit fournir un échantillon des caractéristiques sur lesquelles se base la reconnaissance. Cette procédure (appelée enregistrement) permet de créer un modèle des caractéristiques retenues (l'image des empreintes digitales par exemple). La vérification biométrique est la comparaison du modèle mémorisé sur la carte et des caractéristiques présentées par le détenteur. Toutefois, ces technologies sollicitent davantage la mémoire de la porteuse. Cette identification sans danger convient mieux aux autorisations hors ligne, l'image du signe biométrique étant enregistrée sur la puce et non pas dans le système central. Avec l'identification biométrique, le détenteur de la carte n'a pas à mémoriser quoi que ce soit (chaîne alphanumérique, code personnel, numéro d'identification, etc.). Cette signature ne peut être devinée ou cassée.

  Concernant l'authentification entre la carte et le système connecté, on applique les règles habituelles en matière de réseau, grâce à la puissance de calcul du micro-ordinateur monté sur la puce.

APPLICATION DES CARTES A PUCE

Les cartes à puce offrent toute une gamme de possibilités en matière de gestion de transactions impliquant l'utilisation de données à caractère personnel. Elles facilitent par conséquent le traitement de ces données dans de nombreux domaines d'application sensibles. La fonction élémentaire d'une carte à puce est de stocker et de transmettre des données, ainsi que de permettre

un échange d'informations entre les différents composants individuels du système d'information global de l'application considérée.

Les cartes à puce sont détenues par des citoyens qui les considèrent comme un bien privé, personnel et sûr, placé sous leur contrôle. Les cartes à puce peuvent servir d'élément clé en offrant une interface conviviale et sécurisée avec les services requis, ainsi qu'un accès aux informations personnelles stockées dans l'application (le système d'information).

De nos jours, les cartes à puce sont utilisées dans de nombreux secteurs : commerce de détail (paiement électronique, cartes de fidélité), télécommunications (cartes SIM, GSM), banque (transactions de paiement), sécurité (contrôle des accès), transport (péage d'autoroute, tickets de parking ou d'autobus/tram, achat de carburants), santé (fiche médicale, données professionnelles, pharmacie), administration (transactions entre les citoyens et les organes gouvernementaux, clés pour signature électronique), etc.

Aujourd'hui, cependant, on ne classe plus les applications de carte à puce selon le secteur d'activités visé mais plutôt en fonction des contraintes techniques et de sécurité à respecter. Une douzaine de catégories essentielles ont ainsi pu être identifiées lors d'un vaste débat sur les nouvelles technologies organisé dans le cadre de l'initiative eEurope :

Identité publique

Le but est de parvenir à un document européen commun d'identification numérique des citoyens. Pour cela, un certificat adéquat de citoyenneté[13] est requis. Ce document marquera une étape capitale dans l'avènement du «e-government» (administration en ligne) dans les États membres. L'un de ses avantages tient au renforcement de la sécurité des données. En général, les cartes à puce permettent d'instaurer une relation unique entre le citoyen et l'Administration de son pays.

Identification et authentification

Le but est de contribuer à créer une plate-forme de sécurité commune, praticable et abordable pour toutes les transactions électroniques requérant une identification et une authentification.

La priorité est accordée aux infrastructures PKI (voir la note 7) et aux cartes à puce lorsqu'il s'agit de prendre en charge des services fiables requérant des fonctions d'identification, de signature numérique et de confidentialité.

Profils de protection, certificat de sécurité

Le but est d'élaborer la norme spécifique et de faciliter ensuite son adoption[14] (via l'industrie de la carte à puce) aux fins de l'évaluation et l'homologation des produits et systèmes, de manière à inspirer confiance aux utilisateurs de cartes à puce.

Lecteur de carte universel

Le but est de définir les caractéristiques architecturales des terminaux de carte universels. Ces fonctions unifiées assurent l'interconnexion sécurisée des cartes à puce avec des réseaux ouverts, quel que soit le type de la carte et de l'application.

---

[13] Ce certificat permet une authentification certaine du citoyen, le cryptage des données et l'utilisation de signatures numériques

[14] Critères communs (CC) - ISO/CEI 15408

Paiement électronique et paiement mobile[15]

L'objectif prioritaire est l'adoption des cartes à puce comme moyen sûr de paiement. Cette application exige bien entendu une bonne interopérabilité entre les canaux, les secteurs et les pays.

Cartes à puce sans contact

La technologie des cartes à puce sans contact sera largement utilisée dans le commerce électronique ou mobile, ainsi que dans les transports publics. Les règles et réglementations adoptées devront concilier les intérêts des constructeurs et ceux des utilisateurs finals.

Cartes à puce multiapplications

Le but est d'accroître la liberté de choix du citoyen amené à sélectionner et à utiliser des services TIC (Technologie de l'Information et de la Communication). La carte à puce semble être le meilleur jeton d'accès générique. L'objectif est de parvenir à un cadre pour des plates-formes ouvertes de cartes à puce (multiapplications et interopérables) faisant l'objet d'un strict contrôle de sécurité.

Les cartes multiapplications requièrent une coordination technique de tous les composants : carte à puce, technologie des microcircuits intégrés, système d'exploitation et activités de gestion.

Transports publics

Le but est de favoriser les transports publics en utilisant la carte à puce comme jeton d'accès. Cette application requiert également l'interopérabilité des systèmes de billetterie utilisant des cartes à puce.

e-government (administration en ligne)

Le but est de définir, rationaliser et mettre en place un modèle européen de procédures administratives reposant sur l'utilisation de cartes à puce. Ceci, afin surtout de promouvoir l'utilisation efficace des sources d'information gouvernementales, l'accès aux services publics et la simplification de certaines procédures administratives. L'utilisation d'une signature électronique, d'une infrastructure PKI et de l'Internet sont des conditions indispensables.

Soins de santé

Les soins de santé furent l'une des premières applications de la carte à puce. L'objectif des activités conjointes des Européens est de parvenir à une bonne interopérabilité des cartes à puce informatives employées dans le domaine des soins de santé, des services d'urgence, de l'assurance maladie et sociale, de la pharmacie, etc. Il est nécessaire de bâtir un cadre législatif, normatif et éthique régissant le fonctionnement des systèmes d'information médicale reposant sur l'utilisation de cartes à puce. Cette condition vise aussi bien les cartes des patients que celles des professionnels de la santé et leur utilisation au sein d'un réseau. Les données couvertes sont à la fois administratives et médicales, de sorte que certains voient dans cette activité la juxtaposition de trois cartes différentes dotées chacune de leurs propres fonctions (par exemple : carte d'identité, carte de signature et carte de santé) mais pouvant bien entendu être regroupées physiquement en une seule.

---

[15] En anglais «E-payment» et «M-payment».

Signature électronique avancée

La signature électronique constitue un nouveau domaine d'application des cartes à puce. Le but est de permettre aux citoyens européens d'exécuter en confiance et sans restrictions, sur des réseaux ouverts tels que l'Internet, des transactions relevant de divers domaines.

SPÉCIFICITÉ DE LA CONSERVATION, DE L'ACCÈS ET DU TRAITEMENT DES DONNÉES

L'utilisation de terminaux de carte et de cartes à puce polyvalents et multifonctions rend désormais abordable l'introduction de technologies modernes mais chères. Elle pose cependant des problèmes spécifiques relatifs à la manière de partager les ressources techniques sans pour autant générer des conflits entre le stockage et le traitement des données. En outre, aucun conflit ne doit venir perturber l'exécution d'une procédure externe essentielle telle que la fusion des données provenant de diverses bases de données (juste avant la personnalisation de la carte), la supervision de la circulation et des plaintes des clients, ainsi que la distribution des clés cryptographiques aux cartes et aux terminaux.

De ce point de vue, il est possible de distinguer entre trois modèles basés sur le choix et la gestion des applications de carte à puce :

Modèle centré autour de l'émetteur

Ce modèle confie l'administration exclusive des diverses applications à l'émetteur de la carte. Parmi les exemples contemporains, citons les systèmes bancaires dans lesquels la banque possède à la fois la carte et les données qu'elle renferme, de sorte qu'à beaucoup d'égards le client (le titulaire) peut être considéré comme détenant celle-ci en prêt. C'est la banque qui décide des données figurant sur les cartes (et les terminaux) et des modalités de leur enregistrement, le client étant tenu de se plier aux règles d'utilisation du système. Il peut cependant refuser de l'utiliser.

Sur le plan conceptuel, ce modèle peut être considéré comme une extension du système d'information bancaire courant au moyen d'un sous-système auxiliaire à carte.

Il ne convient pas aux systèmes obligatoires, dans la mesure où si l'on contraint le titulaire d'utiliser une carte particulière, il doit au moins avoir la garantie que ses données à caractère personnel seront protégées.

Modèle centré autour du fournisseur de service

Ce modèle repose sur la décision de certains organismes émetteurs, surtout les opérateurs GSM avec leurs cartes SIM, d'autoriser l'utilisation de leurs cartes pour acheter des services à d'autres fournisseurs et pour les payer (par exemple en cas d'achat sur des distributeurs automatiques ou dans des laveries automatiques de voitures à l'aide d'une carte SIM, ou bien en cas d'utilisation d'applications prépayées, etc.).

La sécurité de cette solution repose sur la qualité de l'identification racine (SIM) et de la protection des transmissions GSM, ce qui limite la sécurité des autres applications.

Dans ce modèle, cependant, la menace d'une fuite des informations est bien réelle. Depuis une application GSM, il est impossible de déterminer par exemple ce qu'un individu achète personnellement via la carte SIM de son téléphone. Il est par contre possible de localiser

précisément l'endroit et l'heure de ses achats. Un problème typique a trait à la mise en œuvre technique des serveurs sur lesquels ces applications (GSM) s'exécutent. Il s'agit d'ordinateurs très rapides, équipés de bancs de mémoire et autorisant le traitement ultrarapide de plusieurs transactions concurrentes. D'autre part, ils accumulent une quantité énorme de données de valeur inégale : certaines sont requises pour le fonctionnement du système GSM lui-même, d'autres pour le traitement appliqué par les fournisseurs de service supplémentaires.

Des entrepôts de données efficaces peuvent donc être mis en place en vue de permettre une exploration en profondeur de l'information recueillie. Cette activité doit être considérée comme risquée et requiert une supervision en matière de protection des droits de l'homme. Le danger principal réside dans le fait que les données sont communiquées via des canaux groupés d'où elles pourront éventuellement être extraites à l'insu du fournisseur de service.

Modèle centré autour du titulaire

Ce modèle est plus ou moins en usage dans les régions nordiques. Dans les cas extrêmes, la partie intéressée reçoit une carte à puce gratuite (ordinateur de poche) et, via un terminal, kiosque ou autre nœud sécurisé, sélectionne elle-même les applications qu'elle désire avoir sur la carte : identification de citoyen, certificat autorisant la signature électronique, assurance maladie/sociale, portefeuille électronique, cartes prépayées ou de fidélité, banque à domicile, etc.

Dans ce cas, le titulaire est à la fois propriétaire de la carte en tant qu'objet et des données qu'elle contient. Sa capacité à les utiliser et à les gérer dépend d'une infrastructure préexistante composée (de haut en bas) des éléments suivants :

- une définition des dispositions de la législation applicable visant les pratiques généralement acceptées (par exemple, protéger le numéro d'identification personnelle et ne pas l'écrire sur la carte) ;
- l'infrastructure des nœuds de connexion, à savoir les terminaux pour cartes ;
- les applications logicielles disponibles pour les terminaux et pour les cartes elles-mêmes, sous forme d'applets (miniapplications) enfichables ;et
- la plate-forme technologique, qui représente l'aspect le moins problématique ; jusqu'à présent, en effet, nous sommes incapables d'utiliser efficacement, rationnellement et en toute sécurité les fonctions techniquement possibles.

Risques particuliers au traitement des données à caractère personnel au moyen de cartes à puce

Le volume croissant des données enregistrées dans les mémoires des cartes augmente les risques d'attaques contre ces cartes ou contre les données qu'elles contiennent. En conséquence, la demande de protection des informations contre tout accès ou tout traitement non autorisé des données à caractère personnel se fait plus forte. On peut dire que le succès des systèmes reposant sur l'utilisation de cartes à puce dépend de la protection des données enregistrées sur ces cartes.

L'un des risques les plus importants liés à l'utilisation des cartes à puce est le traitement de données sensibles à caractère personnel. Si des données sensibles concernant le détenteur de la carte ou les membres de sa famille sont enregistrées sur la carte, il ne faut jamais perdre de vue qu'un certain nombre de personnes autorisées ont accès à ces données, de même que d'autres personnes en cas de piratage de la carte. Lorsque les droits d'accès aux données sont définis (par exemple à l'aide de la carte attribuée aux membres du personnel), il est difficile de personnaliser précisément l'étendue de ces droits.

Les applications permettant les opérations de paiement (cartes de crédit, porte-monnaie électronique, carte à pré-paiement) présentent un risque particulier de fraude à la carte à puce. Ces cartes sont souvent l'objet de fraude et sont devenues la cible d'individus souhaitant utiliser ces cartes pour s'approprier le bien de leurs détenteurs (essentiellement l'argent). Si ces fonctions financières sont combinées à d'autres (cartes multifonctions), toute utilisation frauduleuse d'une carte pour se procurer de l'argent permet du même coup d'accéder aux autres données à caractère personnel, y compris les données sensibles, enregistrées sur celle-ci. Ainsi, au risque originel s'ajoute un risque supplémentaire découlant de la connaissance indue de données à caractère personnel sensibles. Ce risque peut toutefois être prévenu en ne couplant pas les fonctions de paiement avec des données à caractère personnel sensibles sur des cartes multifonctions.

Pour ces raisons, certaines données à caractère personnel sensibles ne devraient pas du tout être enregistrées sur des cartes à puce. C'est par exemple le cas des données relatives à l'origine raciale ou ethnique, à l'appartenance religieuse, à l'orientation sexuelle. Dans certains pays, la loi interdit l'enregistrement de ce type de données sur les cartes à puce.

Une attention particulière doit être portée aux cartes de santé si des données à caractère personnel concernant l'état de santé du détenteur de la carte ou des membres de sa famille sont mémorisées dans la puce. Le débat est toujours ouvert en ce qui concerne la nature des données à inclure dans ces cartes. Aucune norme n'a encore été adoptée, ce qui fait que chaque pays a défini de son côté les données sanitaires à caractère personnel utilisées par son système (la plupart de ces systèmes en sont encore au stade expérimental ou en phase d'essai). Dans les applications du secteur de la santé, la carte à puce est utilisée comme moyen d'accès aux données sur la santé, lesquelles sont stockées en un lieu donné (généralement chez le médecin traitant ou le médecin de famille, à l'hôpital, etc.)[16], ou comme support pour des données relatives à la santé du patient (du détenteur de carte) et sélectionnées dans son dossier médical.[17] Il n'est donc pas souhaitable d'allier sur une même carte à puce, dans le cadre d'un système multifonctions, des données concernant la santé à des fonctions de paiement ou à d'autres fonctions sans rapport avec la santé ou les services sociaux, l'assurance, santé, la sécurité sociale, etc.

La protection des données à caractère personnel est liée à la solution de deux problèmes :

Accès aux données à caractère personnel

La question de l'accès aux données à caractère personnel enregistrées sur les cartes à puce comporte deux aspects distincts :

- l'accès par le détenteur de la carte
- l'accès par un tiers.

Le détenteur de la carte a toujours la possibilité de lire les données enregistrées sur sa carte. Cette approche repose souvent sur l'installation de guichets publics qui permettent au détenteur de la carte de consulter confidentiellement les données qu'elle contient.

L'accès à ces données par un tiers est un problème plus compliqué du point de vue de l'application. Il est nécessaire de constituer des groupes de personnes autorisées à consulter les données à caractère personnel et de leur attribuer des autorisations plus ou moins étendues. Un groupe donné aura par exemple l'autorisation d'accéder à un ensemble de données limité ; un autre groupe pourra avoir accès à toutes les données ; certaines personnes ne pourront que consulter les données alors

[16] En principe, la constitution de bases de données contenant des informations sur la santé des patients et dont l'administration est assurée par une entité ne relevant as du secteur de la santé n'est pas acceptable.
[17] Comme les données nécessaires en cas d'urgence.

que d'autres pourront les modifier, les compléter et les mettre à jour. Différents niveaux d'autorisation sont généralement attribués à ces tiers au moyen de cartes dites professionnelles.[18]

Adoption d'une cryptographie fiable

Une méthode importante pour assurer la sécurité des données repose sur la sécurité des logiciels. Celle-ci a bénéficié des méthodes de cryptographie grâce à l'incorporation de microprocesseurs spécialisés. Pour parvenir à un haut degré de sécurité, les cartes à puce encryptent les données en utilisant les techniques de cryptographie à clé publique (PKT). Celles-ci permettent à deux entités de communiquer de manière à ce qu'un tiers ne puissent pas lire, déterminer ou modifier les données transmises au cours d'une transaction en ligne, par exemple entre le lecteur de cartes et la base de données centrale). La signature numérique est l'une des applications du système PKT.

Notification

Les applications fonctionnant avec cartes à puce concernant un nombre croissant de personnes. La mémoire des cartes à puce permet d'enregistrer des quantités de données à caractère personnel et autres toujours plus importantes. La mauvaise application des mesures de sécurité comporte des risques pour la vie privée des détenteurs de carte. Il est donc recommandé que les applications reposant sur l'utilisation de cartes à puce soient notifiées aux autorités de contrôle nationales.

II. ASPECTS JURIDIQUES

Les cartes à puce n'offrent pas seulement un certain nombre d'avantages dans le domaine des communications électroniques. Elles comportent aussi certains risques pour les particuliers, surtout dans la mesure où elles permettent de reconstituer les transactions effectuées et de s'immiscer ainsi dans la vie privée de leur titulaire. Ces considérations soulèvent de nombreuses questions législatives. Il est rare que l'on sache exactement qui est le «propriétaire» des données à caractère personnel enregistrées sur la carte, qui est responsable de leur complétude et de leur exactitude ou qui est chargé de la sécurité de la carte et du système.

La question de la propriété des données à caractère personnel enregistrées sur une carte ne se pose pas. Des discussions à ce sujet ne doivent pas être acceptées. Le détenteur d'une carte reste à tout moment en possession de celle-ci et exerce un contrôle total sur les informations le concernant. Les données à caractère personnel doivent être accessibles sans se soucier de qui les a collectées et inscrites sur la carte ou dans la microplaquette. Les relations entre le détenteur de la carte et d'autres personnes qui collectent et inscrivent des données à caractère personnel sur la carte ne doivent limiter en aucune manière l'accès aux données par la personne concernée.

En cas de recours aux cartes à puce dans le cadre d'une application traitant des données à caractère personnel, il est donc nécessaire d'énoncer des règles législatives, éthiques et autres pour protéger ces données contre un accès, une modification ou une exploitation illicite. La portée et la rigueur de ces règles augmentent en même temps que le nombre d'applications utilisant de telles données.

[18] Une carte professionnelle est une carte à puce permettant de coordonner l'accès de tiers à des données à caractère personnel. Le logiciel lit d'abord les données enregistrées sur la carte professionnelle et, en fonction de l'identification de ce tiers concerné et du niveau d'autorisation dont il bénéficie, lui permet de procéder à diverses opérations avec la carte du détenteur.

Les cartes multiapplications hébergent davantage de données à caractère personnel et accroissent par conséquent le risque d'usage illicite et d'atteinte à la vie privée.

La prolifération des applications inhérente aux cartes à puce multiapplications rend également nécessaire la définition juridique de certains droits et responsabilités. Dans le cas des cartes à puce multiapplications, il apparaît indispensable d'énoncer notamment les droits et obligations de l'émetteur et du titulaire des cartes, ainsi que des organismes contrôlant leurs données. Dans le cas des cartes monoapplication, par contre, il semble possible de poser les règles sans recourir à des lois (par exemple en adoptant des règlements internes, des codes d'éthique, des normes, etc.).

La majorité des applications de carte à puce contiennent des données à caractère personnel visant une personne identifiée ou identifiable. Elles contiennent également de nombreuses données et informations sensibles relevant de la sphère intime du titulaire. Il est donc nécessaire de légiférer pour garantir la protection et la confidentialité des données concernées. Les principes fondamentaux en matière d'utilisation des cartes à puce répondent à plusieurs exigences :

1. Adoption des principes posés par la Convention n° 108

Tout usage d'une carte à puce permettant l'identification d'un citoyen et l'utilisation de ses autres données à caractère personnel doit respecter les principes fondamentaux définis en matière de traitement des données de ce type par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108) :

a) Les données à caractère personnel sont obtenues et traitées loyalement et licitement :
   - l'administrateur de l'application (l'émetteur) de la carte ne traite les données à caractère personnel enregistrées dessus que pour des finalités déterminées et légitimes ;
   - l'émetteur de la carte veille à ce que les données à caractère personnel ne puissent pas être fusionnées, quelle que soit la procédure de fusion utilisée ;
   - la carte inclut les données à caractère personnel du titulaire ; aucune donnée enregistrée sur la carte ne peut être utilisée à l'insu du titulaire qui doit, en outre, recevoir des explications sur les applications de carte à puce ;
   - les informations portées sur la carte doivent être transparentes pour le titulaire ;
   - le titulaire doit avoir accès aux données enregistrées sur la carte sous une forme lisible et intelligible ; la méthode d'accès aux données respecte la confidentialité et la vie privée (les données ne sont jamais affichées simultanément en public) ;
   - lorsque la révélation des données s'avère indispensable en cas d'urgence ou bien pour défendre l'intégrité physique du titulaire ou ses biens contre un dommage sérieux, elle doit lui être signalée aussitôt que possible.

b) Les données à caractère personnel enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités :
   - aucune application de carte à puce ne peut employer de données à caractère personnel pour d'autres finalités que celles pour lesquelles elles ont été stockées ;
   - chaque application utilise uniquement les données dont elle a besoin et seulement dans le but pour lequel elle a été créée ;
   - sur les cartes multiapplications, les données à caractère personnel doivent être compartimentées pour chaque application (séparation fonctionnelle) ;

- les cartes à puce ne peuvent pas servir à surveiller une personne ou à réduire ses droits de quelque manière ; toute discrimination doit être exclue ;
- les tierces parties auxquelles certaines données à caractère personnel sont révélées dans le cadre d'une transaction par carte à puce n'ont pas toujours besoin de connaître l'identité précise du titulaire ; dans ce cas, il est suffisant que le titulaire accorde son autorisation uniquement pour la transaction concernée.

c) Les données à caractère personnel doivent être exactes et si nécessaire mises à jour :

- les données à caractère personnel inexactes, incomplètes ou périmées par rapport à la finalité de leur collecte ou de leur traitement doivent être effacées ou corrigées.

d) Les données à caractère personnel 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 :

- l'émetteur de la carte et l'administrateur de chaque application assurent la protection des données à caractère personnel en cas de perte, de vol, de destruction ou d'autre usage abusif de la carte et empêchent sa copie ;
- pour chaque application, des systèmes de sécurité doivent empêcher que des personnes étrangères à l'application puissent accéder aux données.

L'un des principes fondamentaux est que le titulaire est propriétaire des informations stockées sur la carte. Comme nous l'avons vu, le titulaire n'est pas forcément le propriétaire de la carte physique. La propriété de l'information a certaines implications ; le titulaire a le droit de :

- connaître les fonctions et les données figurant sur la carte,
- empêcher l'inscription de certaines données ou informations sur la carte,
- révéler discrétionnairement tout ou partie des données figurant sur la carte,
- supprimer des données ou informations spécifiques de la carte.

Les exceptions aux principes susmentionnés ne peuvent être prévues que par la loi.

2. Législation interne

La minimisation et la prévention des risques inhérents à l'utilisation des cartes à puce ne sauraient relever uniquement de l'émetteur de la carte ou du contrôleur des données. Concernant les applications extensives ou s'étendant à l'ensemble du territoire national, c'est donc le gouvernement, les ministères compétents et les autres institutions étatiques qui doivent assumer un rôle actif (par exemple dans le cas d'une application à l'échelon national de cartes médicales, fiscales, de sécurité sociale, d'assurance, etc.).

Dans le cas d'une application extensive ou s'étendant à l'ensemble du territoire national, il est nécessaire de définir les droits et obligations de l'émetteur et du titulaire de la carte, ainsi que des organismes chargés du contrôle et du traitement des données à caractère personnel, des règles de sécurité, le contenu et l'organisation de l'application, les méthodes de vérification des titulaires de carte, la supervision de l'application et d'autres questions visant toutes les étapes du cycle de vie de la carte. Ces droits et obligations sont définis dans le cadre des principes énoncés par la Convention n° 108 et la législation interne.

3. Normalisation

La normalisation est une forme d'autoréglementation. On retrouve généralement dans chaque norme trois caractéristiques courantes : *elle est consensuelle*, *elle concerne l'ensemble d'un secteur d'activités* et *elle est volontaire.* Le processus d'élaboration d'une norme comprend aussi trois étapes.

Les activités dans le domaine de la normalisation, en dehors de la définition de critères et de paramètres techniques, se concentrent aussi sur d'autres problèmes pratiques. Concernant les applications de carte à puce, l'objectif de ces efforts de normalisation vise également à définir des normes de respect de la vie privée, de sécurité et de protection des données, capables d'intégrer les principes de la Convention n° 108 aux projets reposant sur l'utilisation de cartes à puce. Les activités nationales de normalisation, par exemple, définissent l'étendue et la structure des données, y compris les identifiants nationaux. Elles définissent aussi des normes en matière de collecte, de traitement, d'accès et d'utilisation des données à caractère personnel. Les efforts européens dans ce domaine ont créé les conditions de l'interopérabilité des différentes applications nationales, à savoir qu'elles sont connectables et utilisables dans toute l'Europe. Le rôle principal dans ce domaine est dévolu à l'Organisation internationale de normalisation[19] (ISO) et à certaines organisations spécifiques à l'Europe, telles que le CEN[20], le CENELEC[21] et l'ETSI[22].

4. Code de conduite

L'article 5(a) de la Convention STE n° 108 dispose que les données à caractère personnel faisant l'objet d'un traitement automatisé doivent être obtenues et traitées loyalement et conformément à la loi. Une obligation analogue est énoncée dans la Directive 95/46/CE. Le respect de l'obligation d'obtenir et de traiter les données « loyalement » fait fréquemment l'objet de discussions. L'un des moyens de faire respecter cette obligation est de définir des règles de conduite pour le traitement des données à caractère personnel.

L'essor des technologies modernes, y compris celle des cartes à puce, n'est pas toujours bien accepté par les citoyens. Cette réticence tient notamment à la crainte d'une violation de leur vie privée et à l'utilisation abusive des données à caractère personnel contenues dans les cartes. Les données collectées dans les bancs de mémoire de la carte à puce intéressent à la fois les individus désireux de les détourner et les organismes voyant dans cette technologie un moyen de faciliter leurs activités : instituts de recherche, administration, entreprises commerciales, police, etc.

Les applications de carte à puce sont souvent insuffisamment transparentes pour les citoyens qui ne perçoivent pas toujours leurs avantages et leurs mérites. Le code de conduite précise, sans recourir à la loi, les règles de comportement et le rôle respectif des différentes parties intéressées au projet de carte à puce : le secteur informatique, les fournisseurs de technologie, les émetteurs de carte, les opérateurs de système, les contrôleurs de données, les fournisseurs de service et les titulaires.

Ils s'attachent à régir les liens entre la technologie et son application. Le code de conduite peut être général ou porter sur une application spécifique de la carte à puce (soins de santé, banque, télécommunications, etc.). Le principal effet du code sur les applications de carte à puce est de formuler des principes directeurs visant la collecte, l'utilisation, la divulgation et l'accès des informations, en vue de protéger les données à caractère personnel, la confidentialité de leur traitement et le respect des droits des titulaires.

---

[19] ISO (www.iso.ch)
[20] CEN : Comité Européen de Normalisation (www.cenorm.be)
[21] CENELEC : Comité Européen de Normalisation Electrotechnique www.cenelec.org)
[22] ETSI : acronyme de l'anglais «European Telecommunications Standards Institute» (www.etsi.org)

Le code de conduite est un élément important du cadre de sécurité du projet. Les questions d'ordre éthique ont un impact sur l'acceptabilité générale du projet de cartes à puce par les citoyens (détenteurs de carte). Pour être satisfaisante, la solution retenue doit garantir qu'il n'y a pas de risques pour les libertés et droits fondamentaux des citoyens. Si ces questions et problèmes ne sont pas résolus comme il convient, les citoyens (assurés, patients, etc.) risquent de ne pas utiliser ces cartes, ou seulement dans des situations très limitées. Cette attitude négative et cet accès limité auront aussi une influence négative sur la réussite du projet.

Les applications multifonctions basées sur les cartes et le partage de données à caractère personnel dans plusieurs buts incompatibles ne sont pas uniquement régies par des principes légaux, mais aussi éthiques. Du point de vue éthique, il est nécessaire de parvenir à garantir au détenteur de carte (au citoyen) que les données à caractère personnel le concernant seront utilisées loyalement et légalement. Comment l'assurer que ces données seront lues et traitées uniquement par des personnes dûment autorisées ? Comment l'assurer que la simple lecture des données le concernant ne produira pas des effets juridiques à son égard ? De nombreuses autres questions restent à résoudre car « l'éthique » de l'utilisation des nouvelles technologies est une condition de leur réussite. Le code de conduite décrit les principes d'un comportement «loyal» pour toutes les parties prenantes aux application utilisant les cartes à puce (industrie, émetteurs de cartes, prestataires de services, détenteurs et utilisateurs de cartes).

5. Le Conseil de l'Europe et les instruments de protection des données

La protection des droits et libertés fondamentaux constitue l'une des principales activités du Conseil de l'Europe depuis sa création en 1949. La protection des données est comprise comme entrant dans le cadre du principe de protection de la vie privée et familiale, du domicile et de la correspondance, tel qu'il fut énoncé pour la première fois dans l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (1950). Dans ce contexte, ce droit fit donc l'objet d'une protection plus détaillée avec la Convention n° 108 du Conseil de l'Europe[23] (1981) qui constitue l'instrument juridique fondamental en matière de traitement des données à caractère personnel et a déjà été ratifié par 25 États membres du Conseil de l'Europe et signé par 8 États membres.

Il ne fait aucun doute que les principes en matière de protection des données à caractère personnel énoncés dans la Convention n° 108 s'étendent également aux applications de carte à puce, dans la mesure où celles-ci utilisent, elles aussi, des données du même type. Le traitement des données effectué à l'aide de ces cartes est forcément un traitement automatisé, de sorte que les principes de la Convention n° 108 doivent être appliqués dans tous les cas.

Outre la Convention n° 108, le Conseil de l'Europe a adopté 12 recommandations et 2 résolutions et diffusé 4 publications et quelques rapports sur ses activités dans le domaine de la protection des données. La plupart de ces documents visent un secteur spécifique.

La protection des données à caractère personnel dans le cadre des nouvelles technologies affectant la vie quotidienne des citoyens constitue une nouvelle sphère d'activité pour le Conseil de l'Europe. Les progrès rapides de l'informatique, des télécommunications et des autres technologies modernes soulèvent de nouveaux problèmes liés à leurs dommages potentiels sur la vie privée et familiale. C'est la raison pour laquelle le Groupe de projet sur la protection des données (CJ-PD) concentre ses efforts sur ces sujets. La protection des données à caractère personnel sur l'Internet[24] et la

[23] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
[24] Recommandation n° R(99)5 sur la protection de la vie privée sur Internet

protection des données en relation avec la surveillance[25] sont les deux domaines ayant été couverts jusqu'à présent.

Depuis 1996, le Groupe de projet sur la protection des données (CJ-PD) se penche sur les problèmes liés à la protection des données à caractère personnel dans le cadre de l'utilisation de cartes à puce. Le Conseil de l'Europe a publié le premier document traitant de ce problème en 1985[26].

La liste complète des informations et des documents consacrés à la protection des données est disponible sur le site Web du Conseil de l'Europe.[27]

* * *

[25] Activités sur la protection des données en relation avec la surveillance (rapport et principes directeurs) élaboré par M. Giovanni Buttarelli.

[26] CJ-PD : Problèmes juridiques résultant des documents d'identification officiels lisibles à la machine (MRIDs). Council of Europe CJ-PD(85)3, 1985.

[27] www.legal.coe.int/dataprotection/