

# LE CONTRÔLE DES BIENS PAR LES PUCES RFID et RESPECT DES DONNEES PERSONNELLES

Pr. E. Vigano, Haute Ecole de Gestion de Genève  
& Nicolas Rosenthal, Legal Adviser & Lead Auditor, E-DROIT  
2008

# Contexte

- La généralisation de puces RFID sur les objets tient à plusieurs raisons:
  - meilleure efficacité de la chaîne logistique,
  - état permanent des stocks et bibliothèques,
  - amélioration de la relation « client »,
  - sécurité et lutte contre le vol, la fraude ou la contrefaçon, etc.
- Néanmoins, en ce qui concerne le commerce de détail ou la location de livres, la question juridique des conditions de désactivation temporaire ou définitive des tags RFID et de l'effectivité de cette procédure reste ouverte.

En effet, quels sont les moyens permettant au « consommateur » (dans l'hypothèse favorable où celui-ci aurait été préalablement informé de l'existence d'un système RFID sur l'article acheté/prêté) de s'assurer, lors de chaque nouveau passage dans le magasin/ la bibliothèque (ou dans un réseau commercial partenaire) d'où provient l'article porteur d'une puce RFID, que celle-ci ne sera pas brièvement réactivée pour alimenter une base de données relative aux habitudes de consommation/de lecture du chaland?

# Du point de vue de la protection des données

- Il serait donc souhaitable que les projets RFID sortant du champ logistique et concernant le commerce de détail ou la location de livres soient clairement explicités quant à leurs finalités. Le niveau de protection du consommateur pourrait notamment être sensiblement relevé par:
  - des mesures simples d'information (via une labellisation spécifique du projet RFID),
  - des mesures de data management (via la mise en place de dispositifs techniques garantissant la neutralisation définitive des puces RFID dès leur sortie du magasin/ des bibliothèques).
- De ce point de vue également, devront être nécessairement abordées, par les porteurs de projets RFID, les questions relatives à la sécurité des données, non seulement contenues sur les puces, mais également échangées avec d'autres systèmes. L'utilisation de la voie hertzienne, même à courte portée, n'est pas, en effet, sans soulever certaines interrogations quant au maintien de l'intégrité et de l'interception malveillante des données. C'est alors le droit des communications électroniques qui sera d'application (utilisation du spectre hertzien, brouillages et interférences radio, etc.).

# Problématiques lors de l'intégration des données biométriques aux puces RFID

- L'**immuabilité** des caractéristiques biométriques peut s'avérer en réalité une faiblesse grave.
- En effet, les **données biométriques volées ou perdues ne peuvent plus être remplacées** comme un mot de passe ou un certificat. En cas de perte, l'identification biométrique est compromise pour toujours et n'est plus utilisable.
- L'un des problèmes majeurs des systèmes biométriques aujourd'hui est d'annuler une caractéristique pour que l'on n'en fasse pas un usage abusif. Se tourner vers une caractéristique non compromise n'est qu'une solution apparente car tant que l'identification est effectuée, par exemple, à partir d'un seul doigt, les autres doigts sont encore une solution de rechange. Cela dit, **leur nombre est limité**.

## Principes lors du recours aux RFID dans le secteur privé

- En amont, se pose inévitablement la question de l'interopérabilité des différents systèmes RFID. La montée en puissance des contentieux juridiques relatifs à la défense des brevets présente aujourd'hui un risque non négligeable pour les entreprises qui sont à l'origine des différents systèmes RFID.
- En aval, où les systèmes RFID ont en effet pour conséquence directe, c'est même une condition intrinsèque à leur déploiement, de produire des flux d'informations. Dès lors, se posera la question de la propriété de ces informations.

Ainsi, dans le cas d'une chaîne de logistique "intelligente", plusieurs acteurs auront accès aux informations inscrites sur les puces RFID. Les conditions d'accès et d'utilisation à ces informations devront alors être définies préalablement par la voie contractuelle sous peine de créer d'importantes distorsions de concurrence au profit de certains acteurs (droits intellectuels, protection juridique des bases de données, droit de la concurrence et théorie des facilités essentielles, etc.).

# Les différentes réponses sociétales

- L'acceptation
- L'indifférence
- Le rejet

qui seront apportées à la diffusion massive de systèmes RFID échangeant en apparence des flux d'informations négligeables pris isolément, mais considérables dans **un environnement informatique pervasif**.

## « CASPIAN » aux USA

- Le rejet : « **CASPIAN** » (Consumers Against Privacy Invasion and Numbering) l'association américaine des *consommateurs contre l'invasion de la vie privée et la numérotation*.
- Des marques comme Wal Mart, Procter&Gamble, Exxon-Mobil, Benneton, Philips, Gillette, Max Factor... sont montrées du doigt et se voient contraintes de revoir la stratégie marketing / lutte contrefaçon ou vol.
- Le manque de communication de ces entreprises a provoqué un retour d'image très négatif aux USA.

# Recommandations quant à l'usage des RFID sur de produits culturels (p.ex : les livres, DVD...)

- La pesée des intérêts, la finalité (lutte contrefaçon, marché gris, SAV, suivi « clientèle »...)
- La communication sur les données stockées et diffusées
- Le choix de la technologie RFID (compatibilité ou pas)
- Le choix de l'étendue géographique du projet (rejets aux USA...)
- La possibilité de désactiver le RFID à la demande du Client
- Les systèmes RFID devraient faire l'objet d'une procédure de certification et d'audit en matière de protection des données. Ces systèmes devraient également être évalués sous l'angle des risques avant leur mise en fonction. Un concept de protection devrait être élaboré, définissant notamment les processus de traitement.
- Une politique d'usage et une documentation rigoureuse du système doivent être étudiées.



# WHO, WHY, WHAT ?

## Nicolas Rosenthal

- Fondateur de « e-droit », 9 années d'expériences dans la conduite et la maîtrise de la protection juridique des systèmes d'information dans les secteurs financiers et industriels.
- Accompagnement juridique et organisationnel de la mise en place de normes sécuritaires (ISO 17799, Lead Auditor ISO 27001, ISO 15408, ISO 15489) conformément aux cadres réglementaires et légaux tels que la Loi sur la Protection des Données, Bâle II, Sarbanes & Oxley Act 2002, Gramm-Leach-Bliley Act 1999, Health Insurance Portability and Accountability Act, PCI DSS.
- Expertise technico-légale en matière de dématérialisation et archivage légal dans le cadre de nombreux projets d'informatique bancaire.
- Conseiller technico-légal auprès du PFPD sur la révision de la nLPD et nOLPD.
- Thèse de Doctorat en Droit « Validité de la régulation par l'architecture et de la soft law : réflexion autour de la protection des données personnelles », titulaire d'un DEA en droit, criminalité et sécurité des nouvelles technologies (UNIL-IPSC-HEC) à Lausanne. LLM en droit européen et communautaire des affaires, lauréat des travaux dirigés sur les contrats civils et commerciaux à la Faculté de Droit de Montpellier I. Lauréat du diplôme universitaire Droit Ibérique et Latino-américain. Lauréat de l'Académie de l'Organisation Internationale de la Propriété Intellectuelle.

# Remerciements

**Vous remercie pour votre attention**  
**Reste à votre disposition**

rosenthal@e-droit.ch

T +41 (0)21 866 11 11

M +41 (0)76 332 11 11