



Solidarity, Independence, Democracy

## Démocratie Saràl.

Citoyen, pourquoi ne portes tu pas ton badge ?  
La surveillance est la sécurité !



### L'abus RFID.

Lors de l'inauguration du CeBit 2007, la Commissaire à l'Information, Mme Viviane Reding, a déclaré: " A l'occasion de ma participation au CeBIT, les gens me demandent quel règlement j'entends proposer aujourd'hui ? Pour ma part, je n'en ai aucun à proposer, les RFID ne devraient faire l'objet d'aucune sur-réglementation mais par contre, cette industrie devrait bénéficier d'une certaine existence légale."

Référence:

[http://scenariothinking.org/wiki/index.php/Viviane\\_Reding's\\_speech\\_on\\_ubicom\\_comp\\_during\\_the\\_first\\_day\\_of\\_CeBIT\\_2007](http://scenariothinking.org/wiki/index.php/Viviane_Reding's_speech_on_ubicom_comp_during_the_first_day_of_CeBIT_2007)

Dans un futur proche, nous pourrions être suivis à la trace pour nous être habillés, pour avoir mangé ou pour avoir transporté certains objets ou certains articles précisément programmés dans ce but. Cette technologie a un nom générique: RFID qui vient de l'anglais "Radio Frequency Identification". Les RFID sont des balises, des puces quasi microscopiques dont la taille est déjà réduite à la moitié d'un grain de sable. Elles restent à l'écoute d'une fréquence radio donnée à laquelle elles répondent en retransmettant un code d'identification qui leur est unique. La plupart de ces balises n'ont même pas d'alimentation. Elles puisent directement du signal radio reçu l'énergie qui leur est nécessaire pour retransmettre leur réponse.

La technologie RFID nous deviendra bientôt familière, car elle est destinée à être de plus en plus souvent citée. Toute activité de surveillance est positive lorsqu'elle est fondée. Elle peut se révéler entre autre, utile voire nécessaire – pour

combattre le terrorisme ou la grande criminalité, pour favoriser l'accès aux services publics ou privés et à leurs prestations, pour améliorer la santé publique. Mais une surveillance invisible, incontrôlable où excessive est propice à un climat de suspicion, de détérioration de confiance et peut causer de véritables ennuis à certaines populations : exclusion sociale, discrimination, effets négatifs sur l'espérance de vie. Funestement, l'expansion des méthodes de surveillance du 21ème siècle produit d'ailleurs des situations où les distinctions de classes, de race, de sexe, de provenance géographique et de citoyenneté sont couramment exacerbées voire institutionnalisées.

Des experts prévoient des tests biométriques et psychologiques afin de déterminer les plus aptes des salariés. Ceux qui refuseraient de s'y soumettre, ceux qui seraient considérés comme malades ou inaptes, se verraient exclus.

Comment envisager l'insertion de ces balises d'identification radio dans les cartes d'identité ? Va-t-elle favoriser ou éviter les fausses identités ? Certaines personnes considèrent cette technologie comme un solide garant des droits à la personne, alors que d'autres y voient un véritable cauchemar sécuritaire.

Le Sénateur de Californie Joe Simitian, a présenté en Octobre 2007 ce sujet comme "relevant du *Meilleur des Mondes* de Georges Orwell", déjà d'actualité et qu'il est donc important d'en être conscient dès maintenant. Il n'est pas tolérable que des employeurs exigent que leur personnel soit trassable. Ils existent d'autres moyens pour sécuriser les biens physiques et intellectuels d'une entreprise – et ce, certainement sans atteindre aux droits de la personne. "

Référence:

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=202402856>

L'émission de télévision néerlandaise "Nieuwslicht" a récemment réussi avec la collaboration de l'entreprise de sécurité "Riscure" à craquer et à décrypter le prototype RFID néerlandais de passeport.

En l'occurrence, les données échangées entre le passeport et le lecteur de RFID ont été interceptées et stockées. Un mot de passe a été alors simulé en moins de deux heures sur un PC, permettant l'accès aux empreintes digitales, aux photographies, et à toutes les autres informations, qu'elles aient été cryptées ou non, de la balise RFID, soit suffisamment pour bricoler un clone de passeport. L'astuce, en définitive, provient de l'algorithme utilisé pour générer la clé numérique

secrète d'encryptage des données. Cette clé s'est avérée calculable sachant qu'elle est produite d'une manière séquentielle en se basant sur la date d'expiration du passeport, la date de naissance, le numéro du passeport et d'une sommation de contrôle.

L'avantage inhérent de cette technologie qui s'épanouit dans une forme plus prononcée d'isolement sécuritaire serait d'ailleurs inopérant.

Ref: <http://www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/>

Un consultant allemand en sécurité a en effet, démontré qu'il pouvait cloner les passeports électroniques que les Etats-Unis ainsi que d'autres pays s'apprêtaient à distribuer cette année. Les passeports en question contiennent des identificateurs radio ou RFID, puces, que le Département d'Etat US ainsi que d'autres assuraient pouvoir empêcher toute falsification. Par ailleurs, en Allemagne, Lukas Grunwald, un consultant "DN-Systems" en sécurité et expert en RFID, signale que les données contenues dans les puces sont faciles à copier et que "le design entier du passeport ressemble à un cerveau fêlé." Il affirme que de son point de vue, "tous les passeports RFID sont une vaste perte d'argent. Il n'y a pas du tout d'augmentation de sécurité."

Référence:

<http://www.wired.com/news/technology/0,71521-0.html?tw=rss.index>

Les puces biométriques sans contact RFID incorporées dans le passeport du Royaume Uni sont exactement sujettes aux mêmes risques d'atteintes à la vie privée et à la sécurité de la personne que celles du passeport biométrique des USA. Toutes nous rendent plus vulnérables aux criminels et aux terroristes que leurs concurrentes, les puces à contact qui nous sont très familières, à l'exemple des cartes de crédits, des cartes d'autorisation PIN, etc. ....

Référence:

[http://www.rfidbuzz.com/news/2005/spy\\_blog\\_contactless\\_rfid\\_biometric\\_passports\\_in\\_the\\_uk\\_same\\_risks\\_as\\_us\\_rfid\\_passports.html](http://www.rfidbuzz.com/news/2005/spy_blog_contactless_rfid_biometric_passports_in_the_uk_same_risks_as_us_rfid_passports.html)

Des scénarii légaux cauchemardesques sans

**Êtes-vous certain que la Commission n'utilisera jamais de RFID à votre rencontre ?**

**Êtes-vous certain qu'elle ne l'aurait pas déjà fait ?**



Le sénateur de Californie, Joe Simitian, un principal critique de RFID



Commissaire Viviane Reding, un promoteur de RFID

aucun constat de police deviennent imaginables. De futurs divorces pourront se faire sur la simple production d'un extrait partiel d'un registre de RFID qui prouvera qu'un conjoint se trouvait à un certain endroit à une certaine heure... Les voleurs du futur parcourront les allées avec des détecteurs de RFID dont la recherche sera ciblée sur les balises des équipements domestiques les plus coûteux. Dans tous ces scénarii, l'anonymat diminue.

Les RFID restent cependant utiles et sont porteuses de progrès technologiques. Elles permettent aux points de ventes de diminuer leurs contrôles d'inventaires et les vols, qu'un groupe industriel estime à 50 Milliards de dollars par an. La pertinence de l'emploi des RFID dans le domaine commercial devrait se traduire par des prix plus bas et un choix plus large pour les consommateurs. Et puis, ne serait-il pas pratique de pouvoir attraper quelques articles dans les rayons et simplement s'en aller, sachant que nos achats sont automatiquement débités sur notre carte de crédit RFID (espérons-le) sécurisée ?

Les menaces à l'encontre de la vie privée ne deviennent sensibles que si ces balises RFID restent actives une fois sorties du point de vente. C'est précisément ce scénario qui devrait nous mettre en alerte... car actuellement l'industrie des RFID reste contradictoire sur leur automatisme de désactivation ou d'activation par défaut....

La Commission Européenne a également considéré ces risques.

Référence:

[http://www.cc.cec/home/dgserv/jrc/dwnld/docs/dss/jpr/presentations/200504\\_ep\\_wilikens.pdf](http://www.cc.cec/home/dgserv/jrc/dwnld/docs/dss/jpr/presentations/200504_ep_wilikens.pdf)

Le Commissaire Kallas, dans une communication aux membres de la Commission en mars 2007, a reporté que l'usage de cartes biométriques est à l'étude par la Commission pour l'identification de son personnel.

Référence:

[http://www.cc.cec/sg\\_vista/cgi-bin/repository/getdoc/COMM\\_PDF\\_C\\_2007\\_0797\\_1\\_X\\_X.pdf](http://www.cc.cec/sg_vista/cgi-bin/repository/getdoc/COMM_PDF_C_2007_0797_1_X_X.pdf)