

Votations fédérales du 17 mai 2009

NON au passeport biométrique



Conférence de Presse UDC du Valais romand du 24 avril 2009



Ne vous fichez pas d'être fichés

Représentée par le CN Oskar Freysinger, le conseiller communal d'Hérémence Grégory Logean et le député Eric Jacquod, l'UDCVR a présenté lors d'une CP, vendredi, ses arguments contre le passeport biométrique.

Oskar Freysinger s'est plu à souligner qu'il était indigne de la tradition démocratique de la Suisse de ne pas laisser au citoyen le libre choix entre le passeport traditionnel et le fichage systématique de ses données personnelles. Et de rappeler que jusqu'à présent, seules les empreintes des criminels étaient fichées dans un registre central.

Grégory Logean a rappelé le risque que représente le clonage de données biométriques. Le détenteur d'un passeport ne s'apercevant pas de ce genre de vol, les abus peuvent avoir lieu sans que les autorités soient conscients de la nécessité d'agir. De plus, le fichier central n'est pas exigé par les accords de Schengen et l'Allemagne a renoncé à cette mesure jugée excessive sous la pression de ses citoyens. Eric Jacquod, quant à lui, a expliqué les risques de piratage auquel est soumise la centralisation des données et l'inanité du passeport biométrique en cas de pannes électroniques. Il a aussi relevé que le projet de munir également les cartes d'identité de puces électroniques est en cours et qu'une acceptation du passeport biométrique serait un chèque en blanc pour cette mesure. Il a aussi fustigé le fait que le CF pourra déterminer, sans recours au parlement, à quels tiers il voudra transmettre les données personnelles de ses citoyens.

En raison de toutes ces inquiétudes, l'UDCVR recommande aux citoyens de refuser l'introduction d'un passeport biométrique qui met gravement en péril la sécurité des données et la protection de la sphère privée.

UDCVR

Par son président

Oskar Freysinger

Biopass

Par Oskar Freysinger, Conseiller national

Jadis, on se contentait de prendre les empreintes digitales des criminels. Il fallait avoir commis quelque larcin pour être fiché. De nos jours, il ne s'agit plus seulement de persécuter les bandits, mais de protéger le citoyen honnête ... apparemment contre lui-même. Il faut lui enlever son fusil de milicien, éloigner de lui les centres de décision pour qu'il ne lui vienne pas à l'idée de faire un choix libre, donc peut-être mauvais, et il faut tout savoir sur lui pour mieux pouvoir le guider sur le bon chemin. Le bon chemin étant évidemment dicté par la pensée unique, politiquement correcte, globalisée et aseptisée.

Ayant démantelé le contrôle des personnes aux frontières, on étend ce contrôle à l'ensemble du territoire national, où tout le monde devient suspect, surtout s'il n'a rien fait, car cela prouve bien qu'il pourrait faire quelque chose et devenir ce qu'il est potentiellement : Un criminel.

Donc, on stocke des données. Or, les données, comme leur nom l'indique, sont faites pour être données. A qui et par qui ? Personne ne le sait. Le gouvernement en décidera. Sans passer par le parlement. Ainsi, mes données biométriques risquent de nourrir les fichiers de multiples acteurs économiques qui s'intéressent à mon porte-monnaie, voire de services secrets boulimiques se nourrissant d'informations diverses.

On nous assure que tout cela est sous contrôle, qu'il s'agit de garantir la sécurité et la liberté de voyager.

Mais qui nous protégera des fanatiques de la sécurité ? On sera bientôt tellement sûrs, dans notre prison invisible, ce labyrinthe de haute-sécurité dans lequel les puissants veulent nous perdre pour mieux nous tenir, que la vie elle-même finira par avoir peur de nous.

Certes, nous pourrons nous déplacer comme tous les autres bénéficiaires de la fameuse libre-circulation, ce jeu de chaises musicales servant surtout à déplacer le chômage, fragiliser les classes moyennes, détruire l'économie de proximité et les tissus sociaux traditionnels. C'est ça, la liberté de mouvement : Se déplacer librement d'un job mal payé à l'autre en emportant sa prison avec soi.

Le fichier s'en fiche. Il se contente d'afficher mes empreintes et ma gueule de métèque sur les écrans du monde virtuel. Seulement voilà : l'informatique n'est plus si virtuelle lorsqu'elle informe le monde réel de mes mouvements en me collant ses

tiques et ses puces aux basques. Ainsi, ma sécurité sera prétendument garantie par des données qui, elles, sont très peu sécurisées. Etonnant paradoxe.

Pour ne surtout pas mettre la puce à l'oreille de l'homme nouveau, on la lui colle sur son passeport. Un papier qualifié de bio et métrique. Comme ça, on peut suivre le citoyen à la trace, cloner son identité ou, au besoin, le figer sur une des innombrables cases du Monopoly planétaire s'il devait montrer des signes d'irrationalité.

Pour nous apaiser, on nous dit que le contrôle invisible a déjà lieu, parce que tout le monde utilise une carte de crédit, un portable, un ordinateur. Je veux bien. Mais faut-il dès lors aggraver ce qui est inquiétant en renforçant la source d'inquiétude ? Et aux dernières nouvelles mes empreintes digitales ne figurent pas sur mes cartes de crédit ou mon portable.

Ah, il est beau, le brave nouveau monde bio et métrique. Tout y est mesuré, sous contrôle, fiché, identifié, décelé. Tout y est policé et policier.

Que voulez-vous : Rien de tel que la prévention pour prévenir les gens de trop prévoir le destin qui les attend et qui consiste à n'être qu'une patate crispée dans un paquet de chips. Un sacré paquet, qui permet aux affamés du pouvoir de mieux nous croquer le portrait.

Bon appétit et vive l'anthropophagie virtuelle !

Pour ma part, je préfère conserver le libre-choix de la sauce à laquelle je serai mangé. Bio où pas. Et si vraiment je devais un jour vouloir découvrir l'Amérique, je pourrai toujours demander un visa. Ca m'évitera les puces.

On vous fiche, mais ne vous en fichez pas !

Par Grégory Logean (JUDCVR), Conseiller communal

Quelques aspects techniques

Avec le nouveau passeport, les données biométriques sont enregistrées dans une puce RFID. Cette dernière permet la lecture à distance des informations, sans contact physique avec le passeport. Elle contient des données personnelles (nom, date de naissance, taille, numéro du passeport, etc...), ainsi qu'une photo numérique et deux empreintes digitales du propriétaire du passeport. De plus, ces données sont également intégrées à une base de donnée centralisée, appelée système d'information relatif aux documents d'identité (ISA).

Cependant, la sécurité du futur passeport biométrique est remise en question par des experts suisses en informatique mais aussi en protection des données. Mon collègue, le Député Eric Jacquod, reviendra plus en détails sur des exemples concrets des falsifications et de détournement d'identité.

Pour ma part, je vais me contenter d'un petit exemple. Imaginons qu'un terroriste qui a pu copier le contenu de votre passeport biométrique souhaite se faire passer pour vous. Il suffit d'une vague ressemblance physique, un petit coup de rasoir, et la personne pourrait se présenter avec un faux passeport qui contient votre identité et données personnelles. Comme votre document n'a pas physiquement disparu (vous l'avez encore sur vous), mais uniquement été copié à distance, vous n'allez pas annoncer le problème aux autorités. Ces dernières n'auront donc aucun moyen d'avoir connaissance de ce vol d'identité. Le terroriste pourra ainsi voyager en toute quiétude en se faisant passer pour vous...

Exigences de l'UE instrumentalisées par le Conseil fédéral

Une fois de plus, le Conseil fédéral instrumentalise les exigences de l'Union européenne, pour introduire des mesures qui ne sont ni nécessaires ni souhaitables.

En effet, avec les modifications des articles 11 et 12 de la Loi sur les documents d'identité, le CF prévoit que les données biométriques soient également stockées dans le fichier central de l'Office fédéral de la police. Ceci n'était nullement obligatoire et d'autres pays de l'espace Schengen ont renoncé à une base de données centrale. En Allemagne, un projet similaire à celui du Conseil fédéral avait fait l'objet de vives critiques. Au final, les citoyens allemands ont obtenu la garantie de pouvoir demander une carte d'identité sans empreintes digitales, et celles-ci, une fois prélevées, ne sont pas stockées dans un fichier central.

Au passage, relevons que cette instrumentalisation des exigences de l'UE par nos autorités n'est pas un cas isolé. Dans le Nouvelliste du 29 mars 2009, un haut fonctionnaire de l'Etat du Valais constatait ceci au sujet de l'accord de libre-échange agricole : *"Un voyage de travail effectué en début d'année à Bruxelles nous a permis de rencontrer les négociateurs européens en charge du dossier. Ils nous ont affirmé*

qu'un accord global sur toutes les branches de l'agriculture n'était pas une exigence de l'Union européenne, mais bien une demande de la Suisse."

En supprimant la possibilité pour les citoyens de demander une carte d'identité sans puce électronique, nos autorités ont confirmé que l'un de leurs objectifs consiste à disposer d'un fichier concentrant les empreintes digitales de la population. La Confédération fait ainsi subir à tous les citoyens un régime réservé jusqu'ici aux criminels : le prélèvement et le stockage des empreintes digitales. Ainsi, nos autorités suppriment les contrôles aux frontières et font preuve d'un laxisme en relâchant des criminels dangereux pour s'acharner sur le fichage et d'honnêtes citoyens. Ceci est tout simplement scandaleux ! D'ailleurs, même le Préposé fédéral à la protection des données relève le *"caractère disproportionné de l'enregistrement centralisé"* des données biométriques.

Citoyens, on vous fiche, mais ne vous en fichez pas ! Votez NON au passeport biométrique le 17 mai prochain !

Le passeport biométrique : une passoire !

Par Eric Jacquod, Député au Grand Conseil

Le 17 mai prochain, le peuple suisse va devoir se déterminer sur l'introduction d'un passeport biométrique obligatoire. Des données numérisées (empreintes digitales, photographie) seront enregistrées sur une puce intégrée au passeport et dans un fichier central. L'accès à ce fichier sera réglé par le Conseil Fédéral.

Tout ceci est naturellement justifié par des raisons de sécurité et de conformité à des normes européennes. Cependant, beaucoup d'experts mettent en doute la sécurité et des puces et bien sûr du fichier central. *"Des affaires à l'étranger ont montré que ces bases sont très vite détournées à d'autres fins que celles pour lesquelles elles avaient été conçues"*, prévient notamment le Préposé fédéral à la protection des données Hanspeter Thür.

Sans rentrer dans des querelles d'expert, il est évident que la centralisation de données représente un danger de piratage indéniable. Des exemples internationaux nous le confirment : au Chili l'année passée les données de l'équivalent de la population suisse ont été mises en ligne...

En Allemagne, au Royaume-Uni et aux Pays-Bas notamment, des cas de piratage ont été fortement médiatisés. C'est ainsi que des membres du Chaos Computer Club ont réussi, dans un supermarché berlinois permettant de s'identifier par empreintes digitales pour payer ses achats, à se faire passer pour quelqu'un d'autre, ouvrant la porte à des vols de grande ampleur.

A l'EPFL, l'équipe du Prof. Vaudenay a démontré qu'il ne fallait que quatre heures en présence d'un passeport biométrique suisse pour avoir accès au contenu de la puce RFID par une série d'essais-erreurs, jusqu'à la bonne clé. Il serait ainsi possible de consulter les données à distance. En 2006, l'informaticien Adam Laurie piratait par exemple le passeport anglais utilisant la même technologie et réussissait à cloner les données recueillies sur une autre puce.

D'autre part, le passeport biométrique présente un risque supplémentaire par rapport au passeport traditionnel. En effet, il est présenté comme nettement plus perfectionné que ce dernier. Dès lors, il y a de fortes probabilités pour qu'il soit accepté sans réserve lors des embarquements. Le personnel risque de faire trop fortement confiance en la technologie et négligeant le contrôle visuel de la personne, pourtant seul à même de déceler une différence trop grande entre un visage et une photographie.

D'autre part, il faut être réaliste: le véritable enjeu du projet du Conseil Fédéral est l'introduction de la carte d'identité biométrique. D'ailleurs, dans les comptes de l'Etat du Valais récemment publiés, on peut lire que *Les cartes d'identité biométriques seront, selon le résultat de la votation populaire de mai 2009, introduites au plus tard fin 2011*. Les dangers augmenteront ainsi exponentiellement étant donné que ce document doit être porté en permanence sur soi. Les coûts et les démarches

administratives seront évidemment multipliés puisque ni passeport ni carte d'identité ne pourront plus être délivrés par toutes les communes comme actuellement. D'ailleurs, dans le même document, on précise : *les décisions relatives aux investissements et aux postes supplémentaires ont été suspendus par décision du Grand Conseil dans l'attente des résultats de la votation populaire de mai. [...] L'aménagement des locaux, les installations techniques et l'engagement du personnel devront être prévus dans l'urgence et réalisés en 2009 encore.*

Si le projet du Conseil Fédéral est accepté, il sera considéré comme un chèque en blanc pour la carte d'identité biométrique dont le projet est déjà mis en consultation. Les dangers augmenteront ainsi exponentiellement étant donné que ce document doit être porté en permanence sur soi. Les coûts et les démarches administratives seront évidemment multipliés puisque ni passeport ni carte d'identité ne pourront plus être délivrés les communes comme actuellement.

De plus, l'Arrêté fédéral prévoit que les données du système d'information puissent être transmises à des tiers. De nombreuses entreprises privées (sécurité, transport, aviation) pourraient ainsi avoir accès aux données contenues dans les puces des passeports suisses. sans parler de piratage, lorsqu'on se souvient de la manière dont les noms des titulaires des comptes de l'UBS ont été récemment transmis aux autorités américaines avant que l'autorité judiciaire suisse se soit prononcée, on ne donne pas cher de la protection des données biométriques...

Pour terminer, il me paraît important de relever que le passeport biométrique n'est pas adapté aux situations de pannes. On peut prendre l'exemple d'un blackout ou d'une panne informatique. Le passeport biométrique est dépendant du bon fonctionnement de la technologie contrairement au passeport traditionnel.