



**IDENTITÉ.** Notre vie privée est de plus en plus exposée au regard des autres. Par choix pour ceux qui fréquentent les réseaux sociaux comme Facebook. Mais aussi par obligation si les Suisses adoptent

le **passport biométrique** le 17 mai prochain. Ces empreintes personnelles, qu'elles soient ancrées sur le Web ou les papiers d'identité, représentent, chacune à sa manière, un péril pour notre sphère intime

# Notre sphère privée est en danger

Textes: Julian Pidoux

Dessin: Denis Kormann

julian.pidoux@edipresse.ch

**E**lle semblait intouchable, inébranlable, la vie privée des Suisses. Une intimité que le scandale des fiches, à la fin des années 1980, paraissait même avoir renforcée, rendue presque sacrée. Cette sphère personnelle, si farouchement préservée, commence pourtant à s'exhiber.

D'abord par choix pour ceux qui fréquentent sans retenue les réseaux sociaux, Facebook en tête, et dont les profils livrent nombre d'informations sur l'identité des utilisateurs.

Ensuite par obligation si le peuple adopte le passeport biométrique et ses très contestées empreintes digitales lors de la votation du 17 mai prochain.

A ce sujet, la conseillère fédérale Eveline Widmer-Schlumpf, cheffe du Département de justice et police, déclarait récemment dans une interview accordée au «Matin Dimanche» que «Facebook était plus dangereux que le passeport biométrique».

Alors, la notion de sphère personnelle est-elle devenue une illusion, l'anonymat n'est-il qu'un pâle souvenir et à quels dangers sommes-nous réelle-

ment en train de nous exposer en étalant notre identité?

Pour Sébastien Fanti, avocat spécialisé dans les nouvelles technologies, le péril que les réseaux sociaux font planer sur notre intimité est bien réel.

Sans écarter l'éventualité de voir un jour des passeports biométriques suisses falsifiés, l'avocat valaisan est convaincu que, pour l'heure, les plates-formes comme Face-

book sont plus nocives pour la vie privée des Suisses.

Usurpation d'identité, atteinte à la réputation ou commerce de données personnelles font partie de la palette des risques qui guettent les utilisateurs imprudents. «L'Etat offre tout de même de meilleures garanties de confidentialité qu'une société privée américaine qui n'a pas de siège en Suisse, relève Sébastien Fanti. Et, en cas de problème, vous savez au moins à qui vous adresser.»

## Une inconscience collective

Difficile toutefois de parler de mise en danger de la sphère intime lorsque les utilisateurs des réseaux sociaux ouvrent volontairement une brèche dans leur vie. Une position à laquelle Sébastien Fanti n'adhère que partiellement. Ces sites communautaires permettant notamment de faire circuler des photos à l'insu des personnes qui y figurent.

«De plus, les gens n'ont pas conscience des engagements qu'ils prennent, note l'avocat valaisan. L'article 5 des conditions générales de Facebook stipule, par exemple, que le site est autorisé à trans-

mettre les données de ses utilisateurs aux agences de renseignements et aux services de l'Etat américain.»

Et Sébastien Fanti de conclure: «On ne sait donc jamais quand un détail de votre vie va vous porter préjudice.»

## Montre-moi tes amis, je te dirai qui tu es

Début avril, des chercheurs de l'Université de Cambridge ont publié une étude sur les dangers de Facebook pour la sphère privée. Ils y dévoilent qu'il est facile, malgré un accès limité aux informations des profils, de reconstituer la nature des relations entre les gens.

«Les internautes n'imaginent pas que leurs connexions sont une matière confidentielle, explique Joseph Bonneau, coauteur de l'étude. C'est un élément que les services de renseignements ont compris il y a longtemps. Lorsqu'ils effectuaient des écoutes téléphoniques, l'information la plus intéressante n'était pas forcément ce qui se disait, mais qui appelait qui.»

Des indications personnelles qui, assurent les chercheurs anglais, sont très utiles aux gouvernements, aux cyber-criminels ou aux publicitaires.

## Un passeport qui inspire trop confiance

Pour Stéphane Koch, conseiller en intelligence économique et gestion stratégique de l'information, cette peur de Facebook est exagérée. Et si le réseautage social recèle bien quelques pièges pour l'utilisateur non averti, ces derniers n'ont rien de comparable à ceux du passeport biométrique.

Et pour cause. En volant une identité sur Facebook, rien



ne prouve que les détails fournis par l'internaute soient vrais. «Par contre, poursuit Stéphane Koch, le seul but du passeport biométrique est de vérifier l'identité et de la rendre inimitable. Si vous parvenez à falsifier un document que tout le monde pense inviolable, vous agissez au nom de quelqu'un d'autre à tous les niveaux. Cela veut dire

ouvrir un compte bancaire, acheter des billets d'avion ou traverser des frontières.»

L'expert craint ainsi que les autorités ne donnent trop de crédit à la technologie des futurs passeports. «Si l'Etat parvient à produire une puce contenant des informations biométriques à des millions d'exemplaires, d'autres trouveront les moyens de la craquer», assure Stéphane Koch. Ce dernier se demande enfin qui aura accès à toutes ces informations.

#### **Pas de garanties suffisantes**

Une question de fond que Kosmas Tsiraksopoulos, chef de l'information au bureau du Préposé fédéral à la protection des données et à la transparence,

évoque également.

S'il reconnaît qu'«un passeport biométrique ne livre pas autant de détails sur le quotidien d'une personne que certains profils Facebook, les données qui y figurent sont par contre uniques pour chaque personne». Elles ne doivent pas être collectées inutilement.

Kosmas Tsiraksopoulos se demande surtout si «un Etat de droit ne court pas des risques inutiles en créant une banque des données sensibles sur tous ses citoyens». Alors même que ces informations biométriques ne sont pas indispensables pour une identification sûre d'un individu. ◇

## Hackée, usurpée, exposée, la vie privée ne tient qu'à un fil: des exemples

◆ **USURPÉ** En juillet 2008, l'Américain Mathew Firsht a reçu 22 000 dollars de dommages et intérêts de l'un de ses anciens amis. Après une dispute, ce dernier avait créé un faux profil de Firsht sur Facebook, stipulant qu'il était gay et donnant de fausses informations sur son appartenance politique.

◆ **VIRÉE** En février de cette année, la secrétaire anglaise Kimberley Swann a perdu son emploi. Sur son

profil Facebook, elle a eu le malheur de dire qu'elle trouvait son travail ennuyeux. Une information que ses collègues de bureau ont vue et peu appréciée.

◆ **ÉVINCÉ** Le mois dernier, c'est Sean Aspey, conseiller municipal libéral-démocrate, qui a été évincé de son parti à Porthcawl, au sud du Pays de Galles. Des photos de lui, habillé en nazi lors d'une fête costumée d'anniversaire, ont été postées sur Facebook. ◇

◆ **HACKÉ** En août 2006, Lukas Grunwald, consultant pour une société allemande de sécurité, annonce lors d'un congrès à Las Vegas qu'il a réussi à hacker la puce électronique choisie par le gouvernement britannique pour équiper ses passeports biométriques. Sans endommager le document, il est parvenu à transférer l'information biométrique confidentielle sur une puce vierge.

◆ **EXPOSÉ** En septembre 2008, le

Chili découvre que les données personnelles de 6 millions de personnes se sont retrouvées durant quelques heures sur Internet, après le hacking des systèmes d'informations de l'Etat.

◆ **IMITÉ** En octobre 2008, un groupe de hackers hollandais a montré sur une vidéo comment il a réussi à fabriquer un faux passeport électronique, destiné à recevoir des informations biométriques, avec les données... d'Elvis Presley. ◇