

# Ecrans publicitaires du métro parisien



Metrobus.fr

## Illégalité et illégitimité du système

### Synthèse juridique et technique

Nicolas Hervé  
David Sterboul

Associations : Résistance à l'agression publicitaire - Souriez vous êtes filmés - Big Brother Awards - Robins des Toits - Le Publiphobe

Juillet 2009

# Sommaire

## I - Loi de 1995 sur la vidéosurveillance

- 1- Définition de la vidéosurveillance**
- 2- Possibilités d'enregistrement**
- 3- Finalité du dispositif**

## II - Application de la Loi de 1978 sur l'informatique et les libertés

- 1- Loyauté et licéité du dispositif**
- 2- Légitimité de sa finalité**
- 3- Consentement du public**
- 4- Droit d'opposition**

## III – Collecte de données téléphoniques personnelles via le dispositif Bluetooth

## IV- Évolutions technologiques potentielles

- 1- Ciblage des individus**
- 2- Analyse comportementale**
- 3 - Reconnaissance des individus**
- 4 - Autres évolutions matérielles**

## V- Utilisation du dispositif à des fins d'expérimentations non affichées

## Conclusion – récapitulatif

## Annexes

## **I - Loi de 1995 sur la vidéosurveillance**

Le communiqué indique qu'en première analyse, le dispositif ne relève pas de la Loi du 21 janvier 1995 d'orientation et de programmation pour la sécurité, qui traite notamment des systèmes de vidéosurveillance soumis à l'obtention d'une autorisation préfectorale préalable, puisque les images ne sont pas enregistrées.

### **1- Définition de la vidéosurveillance**

En premier lieu, aucune définition de la vidéosurveillance, à notre connaissance, ne stipule que les images doivent être enregistrées pour qu'un dispositif de caméras soit considéré comme devant relever de cette loi.

Or, à l'époque de la rédaction de la loi, le législateur n'avait sans doute pas prévu ce type de technique de transformation directe en données numériques. Il serait donc peut-être nécessaire que la CNIL se prononce, non pas en fonction de la manière dont la loi a été rédigée à l'époque, mais plutôt à la lumière de ces nouvelles évolutions. Les images ont beau ne pas être enregistrées, les personnes n'en sont pas moins observées et leur comportements analysés par des caméras électroniques.

En outre, nous souhaitons attirer votre attention sur le fait que l'enregistrement de vidéos par ces dispositifs est techniquement tout à fait envisageable. Même s'il y a une telle capacité n'est pas exploitée en continu à l'heure actuelle, elle n'en reste pas moins à disposition. Cette simple caractéristique technique devrait faire tomber le dispositif sous le coup de la loi !

### **2- Possibilités d'enregistrement**

De plus, nous nous interrogeons sur deux aspects qui peuvent nécessiter un enregistrement ponctuel des images :

- selon l'algorithme utilisé pour effectuer la détection des visages, une phase de calibrage peut être nécessaire. Il est ainsi possible que les panneaux doivent être calibrés individuellement en fonction des conditions d'éclairage locales et de la configuration des lieux dans lesquels ils sont installés.
- la validation des mesures d'audience auprès des annonceurs nécessitera très probablement une vérification par ceux-ci du fonctionnement correct des dispositifs. En dehors de tests en laboratoires, une mise en situation en conditions réelles est envisageable.

Ainsi, il est probable que l'afficheur doive procéder à des enregistrements pour s'assurer du bon fonctionnement du dispositif ou en apporter la preuve à ses annonceurs. Même si ces deux situations ne nécessitent qu'un enregistrement ponctuel des images, bien défini dans le temps, il n'en reste pas moins un enregistrement, faisant alors irrémédiablement tomber ces dispositifs sous le coup de la loi de 1995, quelle que soit l'interprétation que l'on veut bien en faire.

### **3- Finalité du dispositif**

La loi de 1995 stipule que l'on peut installer des caméras de surveillance dans les endroits ouverts au public, mais uniquement pour **assurer la protection et la sécurité des biens et des personnes**. Le

législateur a défini les limites strictes du champ d'application à ces critères, dans l'idée de fixer un cadre précis qui ne doit pas être dépassé.

Hors ici, nous ne sommes pas dans la protection et la sécurité des biens et des personnes, mais dans l'analyse des personnes à des fins d'ordre purement mercantile, en aucun cas liées à la protection du public. Si l'on suit l'esprit de la loi, un tel dispositif ne peut donc pas être autorisé.

## **II - Application de la Loi de 1978 sur l'informatique et les libertés**

Le communiqué de la CNIL indique qu'« il pourrait être considéré qu'un traitement de données à caractère personnel, soumis à la loi "informatique et libertés", est mis en œuvre », puisque « si seules des données statistiques sont conservées à l'issue du traitement, il n'en demeure pas moins que celui-ci est réalisé à partir d'images qui comportent des visages identifiables, qui sont des données à caractère personnel. »

Nous partageons cette analyse, qui a plusieurs implications de première importance :

### **1- Loyauté et licéité du dispositif**

#### **CHAPITRE II :**

##### **CONDITIONS DE LICÉITÉ DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL**

###### ***Section 1 : Dispositions générales***

###### **Article 6**

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

#### **CHAPITRE V**

##### **OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENTS ET DROITS DES PERSONNES**

###### ***Section 1 : Obligations incombant aux responsables de traitements***

###### **Article 32**

I - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

2° De la finalité poursuivie par le traitement auquel les données sont destinées

**IV. - Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission**

ationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

Les données anonymisées sont collectées à l'insu des personnes, de manière on ne peut plus déloyale, sans aucune information. Toutes ces dispositions sont violées.

Notons au passage que l'article 10 de la loi de 95 indique de même : « [...] Le public est informé de manière claire et permanente de l'existence du système de vidéosurveillance et de l'autorité ou de la personne responsable. »

Il nous semble que le non-respect de ces dispositions mériterait à lui seul une sanction, ou à tout le moins un blâme de la part de la CNIL.

## 2- Légitimité de sa finalité

### Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

Nous souhaiterions que vous vous prononciez sur la question suivante : **l'instrumentalisation des usagers d'un service public de transport comme des cobayes marketing qui s'ignorent, le tout au service d'intérêts privés, constitue-t-elle une finalité légitime pour ce type de dispositif ?**

Pour les associations, pour un certain nombre de personnalités politiques, et pour une très large majorité du public consulté, la réponse est clairement « non ».

## 3- Consentement du public

### Article 7

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le système ne satisfait à aucune de ces 5 conditions.  
Cette disposition est donc violée, puisque l'on ne demande pas son avis au public.

#### **4- Droit d'opposition**

##### Article 38

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

Ces dispositions ne peuvent dans les faits être respectées par la RATP et la société Métrobus.

### III – Collecte de données téléphoniques personnelles via le dispositif Bluetooth

Extraits de l'article du journal Le Monde : « Enquête : Alex is watching you »  
LE MONDE | 28.11.08 :

Un informaticien néerlandais a créé un système de pistage des appareils équipés de Bluetooth, téléphones, ordinateurs et GPS. D'autres passionnés l'ont aidé à créer un mini réseau d'espionnage amateur.

Alex Van Es, un homme grand et massif âgé de 35 ans, vit avec sa compagne dans un joli pavillon de banlieue à Apeldoorn, aux Pays-Bas. Le jour, Alex est informaticien dans une administration. Le soir et le week-end, il s'amuse à fabriquer un système automatisé capable de détecter tous les appareils dotés d'un émetteur Bluetooth, puis de traiter les informations recueillies et de les publier sur son site Web personnel, [Bluetoothtracking.org](http://Bluetoothtracking.org) : "Pourquoi je fais ça ? Les technologies de pointe me passionnent, surtout leurs usages inédits. Il n'y a pas à chercher plus loin."

Partout en Europe, les téléphones mobiles récents sont équipés d'un émetteur-récepteur Bluetooth, pour faire fonctionner une oreillette sans fil ou échanger des photos et des fichiers avec des amis. De même, les nouveaux ordinateurs portables et les GPS de voiture utilisent le Bluetooth pour leurs connexions sans fil de proximité. Or, une fois que cette fonction a été activée, la puce Bluetooth diffuse en continu deux informations : son "adresse" (un matricule d'identification unique) et le nom de l'appareil dans lequel elle est intégrée.

En outre, de nombreux utilisateurs personnalisent leur appareil en entrant un prénom, un surnom familier ou amusant, ou encore le nom de leur entreprise ou de leur chanteur préféré -, autant d'informations permettant de les identifier, par déduction ou par recoupements. En se promenant un soir de novembre sur le site d'Alex Van Es, on découvre par exemple qu'à 17 h 42 le téléphone mobile Nokia modèle 6310- I, matricule 00.60.57.xx.xx.xx, se trouvait à Apeldoorn, au coin de la rue Hoofd et de la rue Deventer.

Ces derniers mois, ce même Nokia a été repéré par Alex Van Es 237 fois à Apeldoorn, entre 7 heures et 22 heures, mais jamais plus tard. Ce jour-là, le site a permis de suivre les déplacements de 558 appareils Bluetooth. Pour chacun d'entre eux, une page Web a été créée en temps réel, avec une carte Google interactive, un tableau récapitulatif, et un graphique ventilant les localisations par tranches horaires. L'ensemble est mis à jour toutes les dix minutes.

[...]

Alex possède aujourd'hui dans sa base de données plus de 6 millions de détections, portant sur 460 000 adresses uniques. Il ne semble pas se lasser et continue à faire preuve d'imagination. Le Parlement de La Haye a organisé récemment une journée portes ouvertes. En bon citoyen, il y est allé, par curiosité : "Une fois sur place, j'ai réalisé que j'aurais pu entrer avec un portable et un capteur Bluetooth, et scanner les noms et adresses des mobiles et des ordinateurs des politiciens et des journalistes présents dans le Parlement. Et le soir, j'aurais pu aller scanner les rues du quartier des prostituées, pour voir si je retrouvais ces mêmes numéros. Je suis sûr que ce genre d'informations intéresserait les citoyens."

[...]

Avec ou sans Alex, le traçage par Bluetooth semble promis à un bel avenir commercial. On estime que, fin 2008, entre 15 % et 20 % des habitants d'Europe occidentale portent régulièrement sur eux un appareil dont la fonction Bluetooth est activée.

En France, l'agence marketing Majority Report a inventé un système très complexe de comptage et de traçage des clients dans les galeries marchandes et les supermarchés, qui combine des caméras stéréoscopiques, des logiciels de reconnaissance faciale et des capteurs Bluetooth.

[...]

Déjà, des internautes anonymes diffusent des logiciels permettant de pénétrer un téléphone mobile grâce au récepteur Bluetooth, pour recopier ou modifier son répertoire, ou même prendre le contrôle complet de l'appareil. Officiellement, ils servent uniquement à dépanner des appareils défectueux. Mais toutes sortes d'usages sont imaginables.

Yves Eudes

Article complet en annexe 1 et sur : [http://www.lemonde.fr/technologies/article/2008/11/28/alex-is-watching-you\\_1124462\\_651865.html](http://www.lemonde.fr/technologies/article/2008/11/28/alex-is-watching-you_1124462_651865.html)

**Y a-t-il ou peut-il donc y avoir collecte de données personnelles (matricule d'identification unique, nom de l'appareil, date et heure de passage, et autres) lors du passage d'une personne à proximité de l'appareil, ou lors des téléchargements de publicité ?**

Si oui, cela constituerait alors un facteur supplémentaire d'illégalité du dispositif.



## **IV- Évolutions technologiques potentielles**

La recherche scientifique en analyse d'images et vision cognitive est très active depuis une dizaine d'années. La détection de visages orientés face à la caméra est un problème résolu depuis longtemps. On peut aujourd'hui en trouver des implémentations open-source (voir la librairie OpenCV d'IBM par exemple). Ce type de technologie est tellement bien maîtrisée qu'elle est intégrée dans tous les appareils photo numériques récents, pour faciliter le travail de mise au point.

Dans ces conditions, on ne peut que s'interroger face aux capacités de calcul embarquées dans les écrans installés dans le métro. Selon nos informations, ce ne sont pas moins de 4 ordinateurs qui sont installés dans chaque panneau. Nous ne pouvons imaginer que la société Majority Report soit incompétente au point d'avoir mal implémenté des algorithmes standard de détection de visages.

Nous interprétons plutôt cela comme une sur-capacité de calcul, installée physiquement dans les panneaux en vue de l'évolution des fonctionnalités. En effet, l'une des caractéristiques fondamentales de ces dispositifs est leur capacité à être mis à jour à distance. Ainsi, le logiciel embarqué dans les panneaux peut être modifié à discrétion et à n'importe quel moment par l'exploitant.

Certaines analyses sur les usagers du métro sont d'ores et déjà envisagées puisqu'annoncées comme telles. D'autres sont techniquement possibles et nous n'avons aucune assurance qu'elles ne seront pas déployées un jour, d'autant plus que certaines le sont déjà à l'étranger :

### **1- Ciblage des individus**

- déterminer le sexe des passants. Des concurrents de Majority Report mettent déjà en œuvre ce type d'analyse (Quividi, TruMedia). Les taux de reconnaissance sont de l'ordre de 85% [1] / [annexe 2].
- déterminer l'âge des passants. Là encore les techniques actuelles permettent d'estimer l'âge avec la même fiabilité que le ferait un humain [2] / [annexe2].
- déterminer la couleur de la peau. Selon le CNRS, il est techniquement tout à fait possible d'effectuer ce type de mesures. Certaines entreprises françaises sollicitent d'ailleurs les chercheurs pour obtenir ce type d'algorithmes [3].
- déterminer le type de vêtements portés par les passants [4] / [annexe 2] : « D'ici la fin de cette année, nos algorithmes permettront de définir à quel groupe d'âge (enfant, adulte, personne âgée) appartient un spectateur, s'il porte des lunettes, une casquette, un iPod, une cravate, s'il a les cheveux bouclés ou pas ».

### **2- Analyse comportementale**

- analyse de l'expression faciale : analyse automatique des émotions des passants en fonction de leur visage [5, 6].
- analyse de la zone de l'image regardée (oculométrie) : selon M. Maurice Lévy, cette possibilité est déjà mise en œuvre dans les panneaux [7].

### 3 - Reconnaissance des individus

Duan-Yu Chen, Chih-Wen Su, Yi-Chong Zeng, Shih-Wei Sun, Wei-Ru, Lai, Hong-Yuan Mark Liao "An Online People Counting System for Electronic Advertising Machines", IEEE International Conference on Multimedia and Expo (ICME2009)

<http://www.iis.sinica.edu.tw/page/library/TechReport/tr2008/tr08009.pdf>

Ce papier décrit un système complet de comptage des passants devant des panneaux publicitaires. Il contient **un système de reconnaissance** pour éviter de compter plusieurs fois une même personne.

### 4 - Autres évolutions matérielles

Au delà des capacités logicielles, d'autres évolutions matérielles sont également possibles. Par exemple, le couplage de la mesure d'audience avec le captage d'informations identifiantes telles que le passe Navigo ou le Bluetooth est techniquement envisageable.

**Quelles garanties avons-nous que chacune de ces évolutions, et bien d'autres encore, ne seront pas mise en œuvre, dans ces panneaux ou dans d'autres dispositifs ?**

---

[1] Erno Mäkinen, Roope Raisamo, "Evaluation of Gender Classification Methods with Automatically Detected and Aligned Faces," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 3, pp. 541-547, March, 2008.

<http://doi.ieeecomputersociety.org/10.1109/TPAMI.2007.70800>

[2] Xin Geng, Zhi-Hua Zhou, Kate Smith-Miles, "Automatic Age Estimation Based on Facial Aging Patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 12, pp. 2234-2240, December, 2007. <http://doi.ieeecomputersociety.org/10.1109/TPAMI.2007.70733>

[3] « Quand la publicité se prend pour "Big Brother" », *Intelligence économique*, France 24, Samedi 23 mai 2009. <http://www.france24.com/fr/20090523-intelligence-economique-numeriflash-publicite-marketing-video-surveillance>

[4] « Media 6 : acquisition de 100% du capital de chinoise Artium. », *Cercle finance*, 25 mai 2009 [http://www.boursorama.com/infos/actualites/detail\\_actu\\_societes.phtml?num=68ea92acec4d2c859e5657020ad06eca](http://www.boursorama.com/infos/actualites/detail_actu_societes.phtml?num=68ea92acec4d2c859e5657020ad06eca)

[5] « Understanding the emotions of consumers », GfK Group, 3 juin 2009 [http://www.gfk.com/group/press\\_information/press\\_releases/004131/index.en.html](http://www.gfk.com/group/press_information/press_releases/004131/index.en.html)

[6] Innovation : Emotional Tool et FaceDetect se proposent de traquer nos émotions, *Ooh-tv*, 16 juillet 2008 - <http://oohtv.wordpress.com/2008/07/16/innovation-emotional-tool-et-facedetect-se-proposent-de-traquer-nos-motions/>

[7] « Les publicités animées font leur entrée dans le métro parisien », *AFP*, 1<sup>er</sup> décembre 2008 <http://www.e24.fr/hightech/mediapub/article25477.ece/Le-metro-parisien-passe-a-la-publicite-animee.html>

## V- Utilisation du dispositif à des fins d'expérimentations non affichées

Nous souhaiterions enfin attirer votre attention sur un fait passé complètement inaperçu jusqu'à présent, mais qui pourrait avoir de sérieuses implications.

Au moment même où les premiers écrans étaient installés, M. Maurice Lévy, président du directoire de Publicis, propriétaire de Métrobus, et M. Guillaume Pépy, directeur de la SNCF, au sein de laquelle 800 de ces panneaux doivent être implantés, ont été sélectionnés pour faire partie des 7 membres du tout nouveau **Conseil économique de sécurité** mis en place par le ministère de l'Intérieur.

Ceux-ci ont été chargés d'apporter leurs compétences « en vue d'une "approche globale" de la sécurité mêlant les secteurs public et privé », afin de faire « face à un développement des risques et menaces de toutes natures » :

Il s'agira, pour le conseil, de "préparer l'avenir et de réfléchir sur les différentes solutions technologiques envisageables". Trois thèmes ont été retenus par la ministre de l'Intérieur :

1. "Déterminer quels sont les besoins de protection face à la crise économique" ;
2. "Analyser les interventions des acteurs privés, déterminer comment les faire intervenir et coordonner ces interventions face au rôle de l'Etat et des collectivités locales" ;
3. **"Comment concilier libertés et efficacité ?", en partant par exemple du "cas pratique du monde numérique".**

Article complet en annexe 3 et sur :

[http://www.lagazettedescommunes.com/actualite/det\\_artNL.asp?id=32310&supportId=56](http://www.lagazettedescommunes.com/actualite/det_artNL.asp?id=32310&supportId=56)

- nous vous laissons le soin de le traduire de la novlangue en français.

A la lecture de cet article, il n'est donc pas du tout exclu que ces panneaux puissent aussi servir, en parallèle, de système d'expérimentation de nouveaux outils de contrôle des populations.

Des inquiétudes similaires sont partagées aux Etats-Unis concernant les applications de TruMedia, dont la technologie, d'après le New York Times, est issue d'activités de surveillance menées pour le compte du gouvernement israélien [9, 10].

**Nous souhaiterions des garanties claires et écrites de la part de la direction de Métrobus et de Majority Report sur ce point, et, le cas échéant, l'application de sanctions en cas d'absence ou de non-respect de ces garanties.**

---

[9] « Billboards That Look Back », Stéphanie Clifford, The New York Times, 31 mai 2008  
[http://www.nytimes.com/2008/05/31/business/media/31billboard.html?\\_r=1&hp](http://www.nytimes.com/2008/05/31/business/media/31billboard.html?_r=1&hp)

[10] « TruMedia says its facial-recognition billboards will never record video, won't share with cops », Nilay Patel, 10 juin 2008  
<http://www.engadget.com/2008/06/10/trumedia-says-its-facial-recognition-billboards-will-never-recor/>

## Conclusion - récapitulatif

Nous attendons donc une position claire de votre part sur les questions soulevées concernant les points suivants :

- 1 - Loi de 1995 sur la vidéosurveillance, possibilité d'enregistrement et finalité mercantile.
- 2 - Loi de 1978 : loyauté, licéité, finalité, consentement, information et droit d'opposition.
- 3 - Collecte de données téléphoniques personnelles.
- 4 - Evolutions techniques possibles en matière de ciblage et de reconnaissance des individus, d'analyse comportementale et d'interaction avec d'autres technologies.
- 5 - Possibilité d'utilisation à des fins d'expérimentations sécuritaires.

Qui vous serviront de base pour vous prononcer sur l'illégalité et l'illégitimité de ces dispositifs.

## Annexe 1 (3 pages)

Enquête : Alex is watching you

LE MONDE | 28.11.08 | 15h35 • Mis à jour le 29.11.08 | 11h09

**U**n informaticien néerlandais a créé un système de pistage des appareils équipés de Bluetooth, téléphones, ordinateurs et GPS. D'autres passionnés l'ont aidé à créer un miniréseau d'espionnage amateur.

Alex Van Es, un homme grand et massif âgé de 35 ans, vit avec sa compagne dans un joli pavillon de banlieue à Apeldoorn, aux Pays-Bas. Le jour, Alex est informaticien dans une administration. Le soir et le week-end, il s'amuse à fabriquer un système automatisé capable de détecter tous les appareils dotés d'un émetteur Bluetooth, puis de traiter les informations recueillies et de les publier sur son site Web personnel, [Bluetoothtracking.org](http://Bluetoothtracking.org) : *"Pourquoi je fais ça ? Les technologies de pointe me passionnent, surtout leurs usages inédits. Il n'y a pas à chercher plus loin."*

Partout en Europe, les téléphones mobiles récents sont équipés d'un émetteur-récepteur Bluetooth, pour faire fonctionner une oreillette sans fil ou échanger des photos et des fichiers avec des amis. De même, les nouveaux ordinateurs portables et les GPS de voiture utilisent le Bluetooth pour leurs connexions sans fil de proximité. Or, une fois que cette fonction a été activée, la puce Bluetooth diffuse en continu deux informations : son "adresse" (un matricule d'identification unique) et le nom de l'appareil dans lequel elle est intégrée.

En outre, de nombreux utilisateurs personnalisent leur appareil en entrant un prénom, un surnom familial ou amusant, ou encore le nom de leur entreprise ou de leur chanteur préféré -, autant d'informations permettant de les identifier, par déduction ou par recoupements. En se promenant un soir de novembre sur le site d'Alex Van Es, on découvre par exemple qu'à 17 h 42 le téléphone mobile Nokia modèle 6310-I, matricule 00.60.57.xx.xx.xx, se trouvait à Apeldoorn, au coin de la rue Hoofd et de la rue Deventer.

Ces derniers mois, ce même Nokia a été repéré par Alex Van Es 237 fois à Apeldoorn, entre 7 heures et 22 heures, mais jamais plus tard. Ce jour-là, le site a permis de suivre les déplacements de 558 appareils Bluetooth. Pour chacun d'entre eux, une page Web a été créée en temps réel, avec une carte Google interactive, un tableau récapitulatif, et un graphique ventilant les localisations par tranches horaires. L'ensemble est mis à jour toutes les dix minutes.

Ce n'est pas la première fois qu'Alex Van Es se fait remarquer sur Internet. En 1998, il fut l'un des premiers Européens à installer chez lui un réseau de caméras connectées à un site Web, afin que les internautes du monde entier puissent le voir vivre en direct. Il avait fixé sur ses équipements sanitaires et ménagers des capteurs informatiques comptabilisant tous ses gestes quotidiens. Son installation est un peu passée de mode, mais elle fonctionne toujours. Alex sait qu'entre le 20 juin 1998 et le 10 novembre 2008, son réfrigérateur a été ouvert 55 003 fois, pour une durée moyenne de 31,12 secondes.

Avec Bluetoothtracking, Alex est passé à l'observation du monde extérieur. Fin 2007, il installe dans sa chambre à coucher un vieil ordinateur de récupération, équipé d'un logiciel qu'il a écrit sur mesure et d'une clé USB contenant un capteur Bluetooth portant à 20 mètres. Aussitôt, l'ordinateur commence à collecter et à stocker les adresses des appareils Bluetooth de ses voisins et des passants circulant dans sa rue. Puis il loue un serveur aux Etats-Unis pour héberger sa base de données.

Avec un seul point de collecte, les informations restent parcellaires et peu exploitables. Très vite, Alex décide d'installer un autre capteur chez sa mère, qui vit en banlieue, et un troisième chez son frère, en centre-ville. Il en met aussi un dans sa voiture, pour scanner les rues pendant ses déplacements. Un commerçant de la ville lui propose d'en placer un dans sa boutique de plomberie : *"Grâce à ce miniréseau, je pouvais suivre des appareils dans la ville, deviner leur itinéraire, calculer leur vitesse, établir des modèles de comportement, repérer des groupes d'affinités ou professionnels..."*

Mais un jour, le journal local découvre le passe-temps d'Alex et publie une série d'articles très négatifs : *"J'ai expliqué aux journalistes que je ne possédais aucune information nominative, que je ne cherchais pas à identifier les individus, mais ils ont écrit n'importe quoi."* Par prudence, Alex décide alors de ne conserver que deux scanners, chez lui et chez sa mère. Sur Internet, il masque désormais les six derniers chiffres des adresses, ainsi que les noms les plus faciles à identifier. Mais il conserve toujours l'intégralité des informations dans sa base personnelle.

En quelques mois, des milliers d'internautes découvrent le site d'Alex, et quelques-uns suivent son exemple. A La Haye et à Haarlem, deux informaticiens créent leur propre système de traçage Bluetooth et décident de partager leurs informations avec Alex pour enrichir son site et sa base de données. Ils sont bientôt rejoints par un Allemand de Heidelberg, deux Britanniques, un Indien et un Néo-Zélandais. Alex est à présent à la tête d'un embryon de réseau mondial : *"Dès qu'un appareil est localisé dans deux villes différentes, il est marqué d'une croix rouge sur mon site. Nous avons déjà suivi un téléphone autour du monde, depuis la Nouvelle-Zélande, jusqu'à La Haye. Génial, non ?"* Cela dit, il faut se méfier des conclusions hâtives. Quand un téléphone est déverrouillé sans l'autorisation du fabricant, l'adresse d'origine est remplacée par celle de la puce ayant servi à créer le logiciel de déverrouillage : *"Si un téléphone est repéré à Apeldoorn à 13 heures, puis à La Haye à 13 h 01, il ne peut s'agir que de deux téléphones différents, piratés avec le même logiciel."*

Parmi les correspondants d'Alex, le plus actif est celui d'Haarlem, Diederik Meijer, 35 ans, qui habite une rue très animée. Il a acheté un capteur haut de gamme portant à 100 mètres, ce qui lui permet de réaliser entre 400 et 500 détections par jour. Il fait des découvertes amusantes : *"Quand un de mes amis passe près de chez moi, je le repère et je peux l'appeler pour lui dire de venir me voir. Même chose avec mon frère : il habite dans la rue voisine, je sais quand il est chez lui ou pas."*

Diederik imagine à présent une infinité d'usages inédits : *"Récemment, une boutique de ma rue a été cambriolée. Je n'ai pas vérifié, mais si les voleurs ont laissé leurs Bluetooth activés, mon scanner a relevé leurs adresses. Ensuite, la moitié des policiers de la ville sont venus sur les lieux du cambriolage. Si je voulais, je pourrais retrouver les adresses informatiques de tous leurs mobiles, et installer une alarme pour me prévenir quand un policier passe en bas de chez moi."* Diederik a décidé d'écrire un logiciel prêt à l'emploi, qui permettra aux non-informaticiens de créer leur propre système.

Grâce à l'aide de ses nouveaux amis, Alex possède aujourd'hui dans sa base de données plus de 6 millions de détections, portant sur 460 000 adresses uniques. Il ne semble pas se lasser et continue à faire preuve d'imagination. Le Parlement de La Haye a organisé récemment une journée portes ouvertes. En bon citoyen, il y est allé, par curiosité : *"Une fois sur place, j'ai réalisé que j'aurais pu entrer avec un portable et un capteur Bluetooth, et scanner les noms et adresses des mobiles et des ordinateurs des politiciens et des journalistes présents dans le Parlement. Et le soir, j'aurais pu aller scanner les rues du quartier des prostituées, pour voir si je retrouvais ces mêmes numéros. Je suis sûr que ce genre d'informations intéresserait les citoyens."*

Alex a déjà transformé son jouet en application utilitaire. Une société de maintenance d'autoroutes lui a proposé de placer deux scanners à 1 km de distance le long de l'autoroute locale, afin de réaliser une analyse fine du trafic sur une longue durée : *"Ils ne pouvaient pas passer par les compagnies de*

*téléphone. Avec les relais GSM (qui transmettent les communications), la localisation d'un téléphone est très précise quand il est en communication, mais beaucoup moins quand il est seulement en veille. Le Bluetooth est plus efficace." Une fois encore, Alex a travaillé pour le plaisir : "J'ai dû améliorer mon système, pour pouvoir capter des appareils filant à 120 km/h. Mais je ne me suis pas fait payer, je leur ai même prêté mon matériel. Je n'ai pas le sens des affaires."*

Avec ou sans Alex, le traçage par Bluetooth semble promis à un bel avenir commercial. On estime que, fin 2008, entre 15 % et 20 % des habitants d'Europe occidentale portent régulièrement sur eux un appareil dont la fonction Bluetooth est activée. En France, l'agence marketing Majority Report a inventé un système très complexe de comptage et de traçage des clients dans les galeries marchandes et les supermarchés, qui combine des caméras stéréoscopiques, des logiciels de reconnaissance faciale et des capteurs Bluetooth.

En Angleterre, l'université de Bath, en partenariat avec des compagnies de télécommunications, a disséminé des capteurs dans les rues de la ville pour mener à bien une dizaine d'études scientifiques portant sur les flux de population en milieu urbain, les usages des nouveaux outils de communication ou la modélisation de la propagation des virus. Victimes d'une campagne de presse hostile, les chercheurs de Bath refusent désormais tout contact avec les médias, ce qui ne fait qu'exacerber les rumeurs.

Déjà, des internautes anonymes diffusent des logiciels permettant de pénétrer un téléphone mobile grâce au récepteur Bluetooth, pour recopier ou modifier son répertoire, ou même prendre le contrôle complet de l'appareil. Officiellement, ils servent uniquement à dépanner des appareils défectueux. Mais toutes sortes d'usages sont imaginables.

**Yves Eudes**

Article paru dans l'édition du 29.11.08



## Annexe 2 (2 pages)



# Avec Quividi, c'est la pub qui vous regarde

Gilles Musi - - L'Expansion.com

[http://www.lexpansion.com/economie/actualite-high-tech/avec-quividi-c-est-la-pub-qui-vous-regarde\\_126464.html](http://www.lexpansion.com/economie/actualite-high-tech/avec-quividi-c-est-la-pub-qui-vous-regarde_126464.html)

**Un écran publicitaire capable d'adapter le spot en fonction de la personne qui la regarde, c'est possible grâce à une start-up française. Mais si cette innovation séduit à l'étranger, elle a encore du mal à s'imposer dans l'hexagone.**

Les spots publicitaires ne se contentent plus de la télé et du cinéma. On trouve des écrans spécialisés dans la rue, le métro, les halls de gares, les aéroports, les magasins, grands ou petits... Mais la plupart ne font que diffuser des messages selon un ordre préétabli. Aucune possibilité de mesurer l'audience : peu ou pas de valeur ajoutée pour l'annonceur par rapport à un bon vieux panneau publicitaire. Or depuis l'an dernier, une jeune pousse française s'est engouffrée dans la brèche : [Quividi](#).

Les quatre compères à l'origine de cette aventure sont des spécialistes du traitement de l'image. La multiplication des écrans dans les lieux publics ne leur a pas échappé. « Qui dit média, dit besoin de rapport d'audience. Notre technologie permet de dire à ceux qui exploitent ces écrans quand et combien de femmes, ou d'hommes les regardent. Nous rendons ces médias capables de s'adapter à une situation donnée, quand bien même ils sont installés dans des zones bruyantes et dans des conditions de luminosité très variables », explique Olivier Duizabo, cofondateur et gérant de Quividi.

Ces moniteurs, vendus par des intégrateurs partenaires de Quividi, sont dotés d'une webcam généralement dissimulée au-dessous ou au-dessus de l'écran. Cette caméra est couplée à un logiciel qui analyse en permanence les flux vidéo captés dans un rayon de 5 à 6 mètres. C'est à cet instant qu'entrent en jeu les compétences de traitement de l'image de Quividi. Le système détecte la présence de visages humains dès lors qu'ils se tournent vers l'écran, et ne les lâchent plus tant qu'ils restent dans son rayon d'action. Toutes les occlusions - une personne qui passe subitement devant un visage, par exemple - sont gérées par le système. « La reconnaissance s'opère dans 95% des cas en moins d'une seconde et la classification homme/femme est précise à 85% », affirme Olivier Duizabo. Il n'est pas sûr que Big Brother ferait mieux... Le patron de Quividi tient donc à préciser : les images ne sont ni enregistrées, ni stockées, ni même exploitables par une quelconque autorité de contrôle. Seuls sont conservés les résultats de l'analyse permettant la mesure d'audience.

Associé à la liste de diffusion, le système permet alors de déterminer combien de personnes ont regardé un clip en particulier ou de calculer son audience cumulée voire même de basculer sur un mode de diffusion de contenu dynamique. Cette faculté est aujourd'hui simplement mise à profit pour adapter des boucles vidéos selon l'heure de la journée, ou pour diffuser des flashes d'informations. Or,

les séquences de cette playlist peuvent être reprogrammées à la volée et diffusées en fonction du profil des spectateurs présents à ce moment-là. « D'ici la fin de cette année, nos algorithmes permettront de définir à quel groupe d'âge (enfant, adulte, personne âgée) appartient un spectateur, s'il porte des lunettes, une casquette, un iPod, une cravate, s'il a les cheveux bouclés ou pas », précise Olivier Duizabo. Bref, du pain béni pour les annonceurs, diffuseurs, régies et autres sociétés d'études.

La France, pour l'instant, semble toutefois bouder cette innovation. Seuls des hypermarchés se seraient risqués à faire des essais. Sur les 15.000 écrans installés dans des lieux publics, aucun ne dispose d'un dispositif de communication audiovisuelle dynamique. Pour Olivier Duizabo, « Le marché français manque d'intégrateurs ayant favorisé cette technologie. Par ailleurs, le poids de l'affichage traditionnel est très élevé du fait de l'implantation de J.C. Decaux. Enfin, la taille des réseaux est limitée ». Du coup, cette jeune pousse s'est tournée vers l'étranger. « Les déploiements ont débuté en Espagne, Grèce, Grande-Bretagne, à Singapour, ou aux Pays-Bas, à raison de plusieurs centaines d'écrans à chaque fois. Les contrats oscillent entre 100.000 et 300.000€. Il faut compter environ 3 000€ pour une étude simple et 200 € par an et par écran pour de gros volumes », précise le patron de Quividi.

Dans l'hexagone, pourtant, les choses commencent à bouger comme en témoigne cet accord signé cet été avec Médiamétrie: « Ils voyaient arriver ces nouveaux médias sur lesquels ils n'avaient pas de prise. Notre technologie a été retenue et Médiamétrie apporte la méthodologie permettant aux différents acteurs du marché (publicitaires, organismes de contrôle de diffusion, annonceurs,...) d'exploiter ses rapports », précise Olivier Duizabo.

## Annexe 3 (1 page)



Sécurité - 26/01/2009

### **Michèle Alliot-Marie a présidé la 1ère réunion du "Conseil économique de sécurité"**

La ministre de l'Intérieur Michèle Alliot-Marie a réuni pour la première fois le 26 janvier 2009 le "Conseil économique de sécurité" qu'elle a créé en décembre 2008, chargé de lui faire des propositions en vue d'une "approche globale" de la sécurité mêlant les secteurs public et privé. Lors de cette première réunion, la ministre a expliqué que, "face à un développement des risques et menaces de toutes natures, il y a une nécessité de disposer d'une structure indépendante et très diversifiée", a rapporté un membre de son entourage.

#### **Trois thèmes retenus**

Il s'agira, pour le conseil, de "préparer l'avenir et de réfléchir sur les différentes solutions technologiques envisageables". Trois thèmes ont été retenus par la ministre de l'Intérieur :

1. "Déterminer quels sont les besoins de protection face à la crise économique" ;
2. "Analyser les interventions des acteurs privés, déterminer comment les faire intervenir et coordonner ces interventions face au rôle de l'Etat et des collectivités locales" ;
3. "Comment concilier libertés et efficacité ?", en partant par exemple du "cas pratique du monde numérique".

Chaque thème devra être pris en main par un chef de projet désigné au sein du Conseil.

#### **2 réunions par an**

Le conseil tiendra deux réunions plénières par an, dont une "sous forme d'un colloque pour présenter ses travaux et ses propositions", a-t-on poursuivi.

Il est composé de :

- Guillaume Pépy, président de la SNCF ;
- Pierre Giacometti, conseiller en communication et ancien directeur général de l'institut Ipsos France ;
- Maurice Lévy, président du directoire de Publicis Groupe ;
- Bernard Spitz, président de la Fédération française des sociétés d'assurances (FFSA) ;
- Alain Juillet, le "M. intelligence économique auprès du Premier ministre" ;
- Laurent Collet-Billon, délégué général pour l'armement au ministère de la Défense ;
- Alice Guilhon du Hellen, directrice du CERAM (Ecole de commerce et de management).

Avec l'AFP