Pourquoi nous pensons que la CNT ne devrait pas promouvoir l'utilisation des codes-barre et autres codes-à-flasher.

Dans le tract confédéral d'appel à la manifestation du 10 septembre 2013, figurait un code QR, c'est-à-dire un code-barre à deux dimensions que l'on peut flasher à l'aide d'un « smartphone ».

Pour les services de renseignement, il était jusqu'ici impossible de savoir qui avait lu un tract de la CNT.
Il est par ailleurs difficile de repérer un internaute qui visite notre site s'il prend les précautions nécessaires (réseau TOR par exemple).
En revanche, lorsqu'un le code figurant sur un de nos tracts est flashé, cette information est directement rattachée au propriétaire de l'abonnement (comme toutes les informations qui passent par le téléphone portable : appels passés, codes flashés, répertoire, textos, photos, vidéos, agenda, courriels, navigation, etc.). Une mine d'or pour connaître dans ses moindres détails la vie des sympathisants d'une organisation, à la portée de n'importe quel hacker.
En effet, il n'est pas indispensable d'être investi d'une mission gouvernementale pour pirater un téléphone : extrême droite et patrons ont déjà bien compris l'intérêt de ces données.
Mais les gouvernements et leurs forces de répression profitent également de nos mouchards :

En Ukraine, le 21 janvier 2014, tous les détenteurs d'un « objet connecté » localisé à proximité des lieux de protestations ont reçu un message : « Cher abonné, vous êtes enregistré comme participant à un trouble massif à l'ordre public ».

En France, le 24 février 2014, les députés et sénateurs ont approuvé le projet de loi de géolocalisation qui autorise les policiers à utiliser « tout moyen technique destiné à la localisation en temps réel » pour surveiller les déplacements d'un suspect. Il peut s'agir notamment de l'obtention en temps réel des informations de géolocalisation reçues par les opérateurs télécom pour les téléphones, « smartphones », « tablettes » et autres « objets connectés ».

Il ne fait plus aucun doute aujourd'hui que les « objets connectés » sont des outils de renseignement qui font partie de l'arsenal répressif à la disposition des puissants. L'évolution technologique décidée par les industriels puis acceptée par la population offre aux forces de répression des possibilités illimitées en matière de renseignements.

Extrait d'une conférence de Lara Srivastava du service "stratégie et politique" de l'Union Internationale des Télécommunications, le 14/10/2006 à l'observatoire technologique de Genève :
"Je veux greffer sur vous une puce RFID dit le lobbyiste
- Cela viole mes droits, répond le consommateur.
- Je veux greffer sur vous une puce RFID qui est aussi un téléphone mobile, une caméra vidéo et un lecteur mp3 dit le lobbyiste.
- Cool, répond le consommateur."

Chaque fonctionnalité attractive incluse dans un « objets connecté » est un argument, non seulement de vente, mais avant tout d'acceptation. Une personne n'acceptera le risque d'être espionnée qu'en échange d'un certain nombre de fonctionnalités (parler à sa famille éloignée, prendre des photos, écouter de la musique, organiser ses contacts, simplifier la navigation grâce aux codes-à-flasher, etc).

Le code-à-flasher est une des « fonctionnalités attractives » participant à l'acceptation d'un outil de répression.

Il ne serait pas cohérent de la part de la CNT de promouvoir une des fonctionnalités œuvrant à l'acceptation d'un outil de répression, fût-il très répandu et déjà largement accepté.

Le 26/06/1974, le premier code-barre moderne est lu sur un paquet de chewing-gum à une caisse de supermarché de Michigan, USA. Cette technologie n'est toujours pas rentable au 01/09/1981 lorsque le département de la défense des USA impose le marquage de tous les produits vendus à l'armée états-unienne. C'est cet énorme marché qui rend finalement cette technologie rentable.
Le code-barre constitue sans nul doute l'innovation majeure du 20ème siècle en matière d'automatisation de la gestion de la production et de la distribution industrielle.

Mais l'utilité du code-barre de 1ère génération s'arrête une fois les caisses passées. En effet, sa lecture nécessite un scanner coûteux et il est impossible de modifier les informations qu'il contient. Il reste donc à populariser la technologie qui permettra de poursuivre l'automatisation de la gestion des objets et des hommes jusque dans la sphère familiale, la puce RFID.

Le 23/01/1973 est déposé le 1er brevet concernant les puces RFID. Au cours des années 80, les RFID se répandent notamment sur les produits susceptibles d'êtres chapardés (disques, livres...), c'est leur 1ère application à très grande échelle.

Identification des camions de l'industrie nucléaire, puis paiement autoroutier, identification des animaux, contrôle d'accès aux pistes de ski, contrôle d'accès au parking, contrôle d'accès aux transports en commun (carte Navigo), les RFID se sont répandues lentement mais sûrement, et sont déjà presque partout.
Dans les cartes d'identité, dans les téléphones, dans les voitures, dans les cartes d'accès à la cantine, dans les vêtements, dans nos animaux, dans certains humains : cobayes volontaires ou militaires, cette liste n'est pas exhaustive.
Tous les documents et discours émanant des lobbys de l'électronique et des télécommunications convergent dans la même direction : leur objectif à peine voilé à long terme est le puçage massif de la population, si possible en sous-cutané, sinon au travers d'une prothèse omniprésente, le « smartphone »[1].

---

1 Extrait du "livre bleu" (2004) du GIXEL (Groupement des industries électroniques) :
"Acceptation par la population : La sécurité est très souvent vécue dans nos sociétés démocratiques comme une atteinte aux libertés individuelles. Il faut donc **faire accepter par la population les technologies** utilisées et parmi celles-ci la biométrie, la vidéosurveillance et les contrôles.
Plusieurs méthodes devront être développées par les pouvoirs publics et les industriels pour faire accepter la biométrie.
Elles devront être accompagnées d'un **effort de convivialité** par une reconnaissance de la personne et par l'apport de **fonctionnalités attrayantes** :
- Éducation dès l'école maternelle, les enfants utilisent cette technologie pour rentrer dans l'école, en sortir, déjeuner à la cantine, et les parents ou leurs représentants s'identifieront pour aller chercher les enfants.
- **Introduction dans des biens de consommation, de confort** ou des jeux : **téléphone portable,** ordinateur, voiture, domotique, jeux vidéo
- Développer les services « cardless » à la banque, au supermarché, dans les transports, pour l'accès Internet, ...
La même approche ne peut pas être prise pour faire accepter les technologies de surveillance et de contrôle, **il faudra probablement recourir à la persuasion** et à la réglementation en démontrant l'apport de ces technologies à la sérénité des populations et en minimisant la gène occasionnée.
Là encore, **l'électronique et l'informatique peuvent contribuer largement à cette tâche**."

Leur stratégie assumée est de donner envie au plus grand nombre, via tous les conforts que cela peut apporter, de s'approcher graduellement de l'étape délicate du puçage sous-cutané.

C'est cet aspect graduel, la technique du « pied dans la porte », qui nous intéresse concernant les codes-à-flasher. Le code-barre, y compris sous sa forme la plus moderne (code-à-flasher), n'est déjà qu'un objet du passé. C'est une technologie qui est déjà obsolète puisque la technologie RFID est déjà bien plus efficace. Mais le rôle véritable de ces codes-à-flasher est d'habituer l'utilisateur à son utilisation, et au niveau de confort qu'il peut apporter : plus besoin de recopier une adresse, plus de risque de se tromper en recopiant, gain de temps, etc. Il s'agit très précisément du niveau de confort qu'apportera l'"internet des objets", projet en cours visant à relier électroniquement tous les objets entre eux, sur le modèle d'internet.
Le code-à-flasher n'est que la version "discount" de la puce RFID. Facile à imprimer, on le scanne avec un appareil photo. L'évolution inévitable sera le remplacement de ces codes par les puces RFID, on gagnera alors la possibilité de scanner à distance (plusieurs mètres), il sera possible de modifier les informations contenues dans certaines puces, il n'y aura même plus besoin d'action humaine pour flasher car ce sont les objets qui seront programmés pour échanger leurs données automatiquement..

Déjà, certains imprimeurs commencent à inclure des puces RFID dans leurs produits. Encore mieux que le tract à flasher, le tract qui se connecte tout seul à ton smartphone en le passant devant ! Qu'attendons-nous ?

Aujourd'hui, une utilisation de la RFID à très grande échelle ferait encore l'objet de contestations potentielles. Il s'agit donc pour les cartels de l'électronique de la « jouer fine » en propageant tout d'abord une autre technologie moins intrusive qui jouerait le rôle de cheval de Troie, de passerelle entre le code-barre du supermarché et la puce RFID sous-cutanée. Le code-barre à deux dimensions, code-à-flasher, que l'on peut générer, imprimer et scanner avec du matériel de grande consommation, est une technologie qui permet d'« éduquer » les masses au confort que la RFID pourrait leur apporter. Le duo smartphone - code-à-flasher change radicalement l'organisation bureautique de ses utilisateurs, notamment dans la nette diminution de l'écriture, que ce soit avec un crayon ou avec un clavier. Plus besoin de recopier une adresse, le scanner s'en charge. Plus besoin de lire le tract papier dans la rue, on le lira en ligne, sur grand écran à la maison, et il ne risquera plus d'influencer notre comportement durant la manif.

L'utilisation massive des codes-à-flasher dans certaines écoles a déjà pour conséquence directe d'écarter les élèves qui ne possèdent pas d'« objets connectés ». On perd donc le choix d'utiliser ou non ces « objets connectés », qui deviennent alors obligatoires. Les familles sont obligées de se soumettre au caractère totalitaire de l'injonction à posséder un « objet connecté ». Un enfant

sans « objet connecté » pourrait devenir aussi incongru qu'un élève sans cartable. Comment une personne ayant grandi avec un « smartphone » à la main pourrait-elle arriver à s'en passer ? Comment cette personne pourrait-elle se délivrer de son mouchard omniprésent ?

Pour la CNT, avoir une vitrine sur internet est une chose, accepter sans les questionner tous les gadgets décidés autoritairement par le capitalisme en est une autre.

Refuser le "code-à-flasher" aujourd'hui, c'est refuser le degré de confort que les lobbys, les patrons et les gouvernements voudraient nous voir réclamer, refuser un choix qui est déjà fait à notre place, refuser un outil de contrôle total de nos vies.

Il n'est pas l'heure d'essayer d'attraper le train du progrès en s'adaptant aux derniers gadgets en vogue. Nous ferions mieux de commencer à réfléchir à la construction de nouveaux réseaux de communication techniquement indépendants de la surveillance généralisée.