Des puces sous la peau, vraiment ?

Author : Hélène Molinari

Date : 1 octobre 2017

Les puces implantées sous la peau refont régulièrement surface entre les colonnes des faits divers et celles consacrées aux innovations technologiques. Avec elles émergent aussi les mêmes interrogations et surtout les mêmes angoisses liées à un monde où l'humain serait pucé et traqué en permanence. Mais a-t-on raison de s'inquiéter ?

> « *Je me suis réveillé, un pansement sur la main. Il recouvrait une petite blessure dans le pouce et l'index. C'est là que j'ai eu un moment WTF. Où étais-je la veille et que m'était-il arrivé ? Lentement, une suite d'événements a commencé à se former dans mon esprit : des flashs, une foule en délire, l'odeur âcre de l'antiseptique et un homme tatoué avec un injecteur spécial. « Bon, il n'y a pas de marche arrière. Tu voulais changer le monde, alors vas-y ! », avais-je pensé. Et j'ai fini avec une biopuce sous ma peau en quelques minutes.* » Eugene Chereshnev #TheSAS2015

Eugene Chereshnev raconte ici le moment où il s'est fait implanter une puce RFID à l'occasion d'une conférence au Mexique réunissant des experts mondiaux sur la sécurité informatique en 2015. Minuscules, de la taille d'un grain de riz, ces puces mesurent 12x2 mm, lit-on à peu près partout. L'opération n'est pas anodine mais n'est pas non plus un acte chirurgical. Cela correspond en fait à un piercing généralement réalisé par des tatoueurs, sans anesthésie.

En mars 2017, une entreprise belge a ainsi défrayé la chronique en implantant à huit de ses employés une puce pour remplacer leur badge d'accès. La société Newfusion assurait alors que tous étaient volontaires. Nathalie Nevejans est maître de conférence et chercheuse en droit, spécialisée en robotique et technologies émergentes en France. Dans un article intitulé « L'usine connectée. L'Usine à l'ère du numérique sous le prisme du droit » (issu de l'ouvrage *Les objets connectés*, à paraître aux éditions Mare & Martin), elle rappelle que « *les droits fondamentaux de la personne s'opposent à une telle implantation* ». Elle cite d'abord le principe de la dignité de la personne : « *Le salarié serait alors ravalé au rang de simple chose, et serait l'équivalent biologique d'un badge.*"

Newfusion n'est pas la seule à avoir tenté l'expérience. Des boîtes de nuit en Espagne en proposent à leurs clients pour faciliter les paiements et avoir accès aux espaces VIP. Au Mexique, ce sont les policiers qui en ont pour être plus facilement retrouvés en cas d'enlèvements. Dangerous Things, une société spécialisée dans le biohacking, estime à une dizaine de milliers le nombre de ses kits d'implants vendus dans le monde. Une goutte d'eau comparée à la population globale.

De la banalisation à l'anecdote

La technologie RFID a d'abord été militaire avant d'envahir le civil. Leur banalisation date des années 2000 avec des applications courantes pour l'identification et la traçabilité d'objets, de personnes (pass navigo et autres cartes sans contact) et des animaux. Une puce est ainsi devenue obligatoire pour les chiens et les chats dans de nombreux pays. Appelées aussi « tags », elles sont composées d'une antenne associée à une puce en silicium électronique qui permet de recevoir et répondre aux requêtes radio émises depuis l'émetteur-récepteur – chacune contient un identifiant unique et des données – avec une capacité de stockage très limitée. Ce sont les émetteurs qui activent les marqueurs et leur fournissent l'énergie nécessaire.

Depuis une quinzaine d'années, les puces RFID sous-cutanées sont aussi et surtout synonymes de complot mondial. Obama aurait donc prévu d'implanter tous les Américains, oui, tous, via son Obamacare. Jacques Attali, lui, ne s'arrêterait pas aux USA mais voudrait implanter tous les êtres humains. Sans oublier l'implant extraterrestre découvert dans le crâne de Napoléon… Katherine Albrecht, « *The RFID lady* » comme elle aime se surnommer lors de ses « *talks* », est une anti-RFID connue dans les milieux chrétiens américains. Pour elle, la puce RFID n'est ni plus ni moins que la marque du diable mentionnée dans la Bible.

La crainte la plus répandue reste bien sûr celle d'une dictature mondialisée où l'espèce humaine serait traquée en permanence. Sauf qu'en fait… nulle besoin d'une puce sous notre

peau, nos smartphones et objets connectés le font déjà très bien.

Deux entreprises françaises spécialisées dans la RFID interrogées n'en fabriquent même pas et ne semblent pas non plus développer de produit dans ce sens. Claude Tételin, directeur technique du Centre National de Référence RFID, n'y voit lui que du « gadget » et non pas une révolution à venir pour nos sociétés. Non, pour lui, nous ne serons pas tous pucés dans un futur proche et le phénomène restera minoritaire. « *Si on oublie le côté amusant, ça reste une authentification de la personne et nous avons pour cela d'autres moyens sans que ce soit lié à notre corps*. »

Se protéger, mais ne pas (trop) flipper

Même si les puces RFID ne sont pas des GPS, il est tout de même possible de les tracer, à condition d'avoir le bon lecteur. Cédric Lauradoux est chercheur à l'INRIA depuis 2009 et membre de l'équipe de recherche Privatics depuis 2011 : « *De nombreux écueils en terme de sécurité et de protection de la vie privée n'ont pas encore été résolus. Cette technologie est très lente en terme d'adaptation. Il est très facile par exemple de dupliquer des cartes à puce RFID – le matériel est en vente libre pour 400 euros. Il y a eu une étude pour voir l'évolution de cette technologie : le constat était effrayant, depuis 2007, les choses n'ont pas changé.* » En 2016, des élèves de l'INRIA ont travaillé sur les puces utilisées par les enseignants, notamment les cartes d'accès aux bâtiments. Leur challenge était de casser la technologie afin de se rendre dans les zones non autorisées. La copie s'est révélée d'une facilité déconcertante.

« *On propose aujourd'hui des étuis en aluminium pour protéger son pass navigo par exemple,* poursuit l'ingénieur*. Quand on ne l'utilise pas, personne n'est ainsi capable d'y accéder. Mais pour le corps humain, il n'existe pas de cage faraday qu'on pourrait mettre autour de son bras. N'importe qui peut donc y avoir accès*. » Un problème qui pourrait être résolu avec de vrais protocoles de chiffrement. Sauf que cela coûte cher et qu'aucune entreprise n'a la volonté de s'y mettre.

Avec un volume de données de quelques ko, cela ne représente en plus pas grand-chose à voler, pourriez-vous objecter. Sauf qu'elles correspondent directement à notre identité : nom, prénom, date de naissance, adresse… Qui sont reliées à un identifiant unique, véritable clé d'accès à notre existence (travail, loisirs, maisons, etc.). Cette limitation de stockage peut donc avoir des conséquences importantes en cas de hacking ou de vol. La question de l'interopérabilité n'est pas non plus résolue : il n'y a aucun intérêt à avoir une puce sous-cutanée contenant nos informations médicales si tous les hôpitaux de peuvent pas les lire…

Cédric Lauradoux ne voit pas non plus le puçage de la population française (ou mondiale) comme un événement majeur des prochaines décennies : « *On a déjà assez de problèmes avec nos puces non implantées. Nos passeports contiennent des puces, nos téléphones nous tracent déjà et à une distance plus importante que les quelques mètres maximum nécessaires pour lire une étiquette RFID*. » Difficile pour lui, comme pour Claude Tételin, de comprendre l'intérêt d'un tel implant pour un individu. D'autant que, pour le moment, les lecteurs interrogent tout ce qui passe à leur portée. Tout est détecté, mais tout ne donne pas accès et seuls les tags autorisés passent. Rien n'empêcherait aussi de positionner des bornes à tous les coins de rue,

ou, dans une vision moins dystopique, à l'entrée des magasins pour identifier les clients qui vont et qui viennent. Sans s'implanter une puce dans le corps, c'est ce qu'a prévu Amazon avec son supermarché du futur pas si lointain que ça : Amazon Go. Il ne s'agit pas là de technologie RFID quoi qu'on s'en rapproche puisque le magasin sera équipé de capteurs et de caméras. Le client, lui, utilisera son smartphone pour scanner ses produits et les payer.

« *Si la RATP veut garder des traces, elle peut par exemple voir que telle carte bancaire est passée à proximité de telle station de métro, souligne le directeur du CNRFID. On entre ici dans l'aspect légal. La RATP ne garde que ce qui la regarde évidemment, mais technologiquement, c'est possible de le faire. » « La balance penche démesurément du côté des désavantages* », conclut Cédric Lauradoux.

S'expérimenter soi-même

Alors, pourquoi une dizaine de milliers de personnes a fait le choix de s'implanter une puce dans le corps ? Hannes Sjöblad est un biohacker suédois. Aujourd'hui à la tête de Bionyfiken - ONG dont le but est de rassembler les biohackers, DIY-biologistes, *bodyhackers*, *grinders* et passionnés de *quantified self* en Suède -, il est régulièrement invité à donner des conférences sur l'implantation de puces. « *Nous sommes encore à une étape expérimentale,* assure-t-il*. Ces puces peuvent être utiles mais pour quelques personnes seulement.* » Il y voit un parallèle avec les téléphones portables dans les années 1980, lorsque peu de personnes les utilisaient malgré le fait qu'ils ne fonctionnaient pas très bien. « *Il existe des substituts à l'implant qui fonctionnent déjà très bien, comme des cartes, des bagues, etc. La raison pour laquelle j'ai une puce, c'est pour comprendre et être éduqué : comment ça marche et surtout quand ça peut être utilisé contre soi, pour comprendre quand quelqu'un est en train d'en abuser. Le savoir, c'est le pouvoir.* » Son but est donc d'anticiper le moment où les grandes entreprises de tech développeront à plus grande échelle ces puces sous-cutanées. Car pour lui, ce jour arrivera.

En attendant, il expérimente, teste par lui-même les avantages et les inconvénients d'une telle technologie. « *Quand je vais à la gym, je passe ma main sur le lecteur de carte. J'ai aussi accès à mon bureau ou j'active mon smartphone de la même façon. Je ne compte pas m'en séparer et je pense en ajouter prochainement pour tester des versions upgradées*. » N'a-t-il pas peur du vol de ses données ? « *Seul le numéro d'identification unique est lu et seules les entreprises où je me suis enregistré peuvent le lire*. »

Eugene Chereshnev, CEO de Biolink.Tech, a évolué depuis son implantation en 2015. Il travaillait alors pour le Kaspersky Lab, société privée spécialisée dans la sécurité des systèmes d'information. En tant que chercheur, il a documenté son expérience sur le blog de la société sous le titre de « Bionic Man Diary ». Il voulait interroger la synergie entre un organisme vivant et un ordinateur et apporter des retours constructifs pour améliorer les prochaines versions de puces et pour « *ne pas laisser les entreprises être les seuls joueurs* ». Car Google, Apple et Microsoft sont déjà lancés dans la course.

ADN digital

Dans la partie 5 de son journal de biohacker, Eugene listait dix réponses à la question : « À quoi

servent les biopuces [puces sous-cutanées, ndlr] ? »

- ouvre des portes

- remplace son passeport et de son permis de conduire

- remplace toutes ses cartes de fidélité

- plus de porte-monnaie ni de cartes bancaires

- contient son historique médical et ses informations d'assurance et sécurité sociale

- plus de mots de passe, accède à tout avec sa biochip

- commande de tous ses objets connectés

- remplace ses billets de transports

- protection anti-vol de tous ses appareils (smartphone, ordinateur, etc.)

- commande de sa propre armée de robots

Deux ans plus tard, sa perception des puces a changé. Notamment après une autre expérimentation : pendant plusieurs mois, il n'a utilisé que sa biochip et a commencé à enregistrer toutes les données produites : nombre de mots, nombre d'emails, nombre de pas, fréquence cardiaque, distance parcourue… Tout. Ce tracking total lui a permis d'avancer sur le concept d'« ADN digital ». En parallèle de notre ADN biologique, il est la somme de toutes nos données mises en commun et décrit ce que nous sommes en tant que personne : « *Dans la plupart des cas, je pouvais me prédire moi-même, ce qui était bizarre et effrayant à la fois*. » C'est ce qui l'a amené à cette conclusion : « *Ce n'est pas l'usage des biopuces qui doit inquiéter, parce que nous sommes de toute façon dans un monde digital, mais de savoir qui possède nos données. Quand cinq ou six entreprises possèdent l'ADN digital de plusieurs millions de personnes, elles possèdent le pouvoir de manipuler l'humanité. Car les données appartiennent à tout le monde, sauf aux personnes qui les produisent.* »

Eugene est donc devenu opposé aux puces, non pas parce qu'elles ne seraient pas utiles, mais parce qu'elles ne sont pas sûres. « *Il est trop tôt. Il faut continuer d'expérimenter. Sur les 10 000 personnes implantées, il y en a peut-être 100 qui sont des chercheurs. Les autres le font pour le* fun. *Mais c'est incroyablement non sécurisé pour les données – si on s'endort dans le train par exemple, n'importe qui peut venir lire notre puce – et la traçabilité aussi. Il est pourtant fondamental d'avoir en permanence le contrôle dessus. Pour le moment, ce n'est pas possible.* »

Il n'existe en effet aucun moyen actuel pour désactiver la puce sans la retirer : « *Détruire sa puce devrait être le privilège de son propriétaire et de posséder les données produites par la puce*. » Un cadre juridique plus adapté serait donc une des premières étapes pour une possible

généralisation de l'usage de ces puces dans nos vies.

Eugene compte donc conserver la sienne et même l'*upgrader* pour poursuivre les recherches mais aussi pour avoir une légitimité à prendre la parole sur ces questions. Comme il le dit, il est trop tard pour s'inquiéter du fait que des hommes et des femmes s'implantent ou ajoutent des éléments non biologiques à leur corps : cela existe depuis (presque) toujours. En commençant par les prothèses. « *Mais les biopuces seront prêtes lorsque j'en serai arrivé à les recommander à ma famille. Et on est encore très loin d'y être.*