Presses universitaires de Perpignan

Un monde sous surveillance ? | Émilie Labrot, Philippe Ségur

La surveillance de demain : puces RFID et implants sous-cutanés

Anne-Lise Madinier

p. 129-146

Texte intégral

« Dans le monde futur, on s'interrogera sur l'époque où les hommes avaient des bibliothèques, où les livres ne parlaient pas entre eux. »
Marvin Lee Minsky

1 Les technologies de l'information et de la communication (TIC) ont peu à peu envahi notre quotidien, prenant entre autres la forme de téléphones cellulaires ou celle d'ordinateurs portables. Les nombreuses avancées en ce domaine ont permis une miniaturisation de ces technologies sous la forme de puces RFID.[1] Cependant, si la miniaturisation n'est apparue que récemment, le système RFID se manifeste dès la Seconde Guerre Mondiale. Les militaires américains l'utilisaient afin de reconnaître à distance les avions ennemis et guidaient ainsi les missiles sur l'avion ayant une signature ennemie. En 1969, le premier brevet lié à cette technologie est déposé aux États-Unis par Mario Cardullo pour l'identification des locomotives. Dans les années 1970, son utilisation est limitée à la sécurité des lieux dits à risques tels les sites nucléaires. En Europe, la première application de cette technologie dans le secteur privé concerne l'identification du bétail dans les années 1980. De nombreuses utilisations commerciales suivront, notamment dans le secteur des constructeurs automobiles. Enfin, la miniaturisation du système RFID, tel qu'il existe aujourd'hui, sera effectuée par IBM qui intègrera cette technologie dans une unique puce électronique au cours des années 1990.

2 La radio-identification ainsi nommée permet de localiser des objets ou des personnes, en mémorisant et récupérant des données à distance. Le système usité se compose de marqueurs, appelés radio-étiquettes, disposant d'une puce RFID, d'une antenne et d'un ou plusieurs lecteurs. Le lecteur, dispositif actif, émet des radio-fréquences qui vont activer les marqueurs lorsque ceux-ci passeront à

proximité, en leur fournissant l'énergie dont ils ont besoin.

3 La puce RFID est un outil de traçabilité. Cette traçabilité peut être définie comme « la possibilité qu'offrent les techniques modernes, à des fins d'information du public, de suivre pas à pas, en une sorte de « trace » continue, les produits de l'industrie dès qu'ils sont diffusés par le grand et le petit commerce. Ils sont en effet marqués, dès leur fabrication, par une information spécifique qui se maintient tout au long de leur vie en quelque lieu qu'ils se trouvent. On pourra ainsi à tout moment identifier un objet, défini par une information virtuelle que les réseaux électroniques diffusent sur toute la planète, de son origine à sa fin, et du producteur au consommateur »[2].

4 Les radio-étiquettes, plus connues sous la dénomination anglaise de RFID tag et usuellement dénommées sous le sigle RFID en raison de la technologie utilisée, s'apparentent à de petits objets telles des étiquettes adhésives qui peuvent être apposées sur divers produits de consommation. Les applications existantes sont variées. Les passes dits Navigo permettant l'accès aux transports publics dans la ville de Paris en sont équipés, de même que certaines bibliothèques universitaires afin de faciliter les prêts d'ouvrages.

5 La puce électronique peut également être implantée dans des organismes vivants tel le corps humain. Ces dernières sont qualifiées d'implants TIC. Ces implants TIC se scindent en deux grandes familles contenant elles-mêmes plusieurs subdivisions. Il s'agit des implants TIC à visée médicale et de ceux ayant un but de surveillance ou de localisation. A priori, la première catégorie ne pose pas de problèmes éthiques puisqu'elle vise par exemple à pallier les déficiences cardiaques. Néanmoins, il est envisageable que ces implants puissent être détournés de leurs finalités premières, notamment lorsqu'il est possible d'y accéder par réseau. En effet, ces implants peuvent être de différentes sortes. Il existe des implants passifs ne pouvant fonctionner que par le biais d'un champ électromagnétique externe, des implants en ligne dépendant d'une connexion

à un ordinateur externe, et enfin des implants TIC autonomes œuvrant indépendamment d'appareils électroniques externes.

6 Le sujet qui nous intéresse plus particulièrement est celui des appareils de surveillance et de localisation. Les implants de ce type posent de nombreux problèmes tant au niveau juridique que par le truchement des principes éthiques. En cela, il faut les rapprocher des radio-étiquettes qui, elles aussi, portent préjudices à certaines libertés fondamentales. Avant d'aborder ces difficultés, il faut là encore discerner les différents types de puces pouvant être insérées dans le corps humain. Trois catégories semblent se distinguer et méritent une attention particulière. En premier lieu, il existe les puces à lecture seule assimilables à celles utilisées pour la localisation des animaux. Elles pourraient, hypothétiquement, servir à repérer les personnes atteintes de la maladie d'Alzheimer.

7 La deuxième catégorie de puce est à lecture-écriture et contient un certain nombre d'informations qui peuvent être modifiées à distance. Ainsi, si cette puce contient le dossier médical ou encore le casier judiciaire d'une personne et que ces derniers sont amenés à évoluer, il sera possible d'ajouter les informations nouvelles sans qu'il soit nécessaire de retirer l'implant. La dernière puce existante contient une fonction de localisation. Un suivi continu des personnes la possédant deviendrait alors possible par simple appel du bon signal.

8 Il est important de rappeler que les implants TIC sont une technologie émergente et qu'à ce titre, des lacunes importantes existent sur leurs connaissances. Il a déjà été démontré par certaines études que la fiabilité de ces puces n'était pas totale. Il faudra donc analyser les différents risques technologiques de cette science intrusive. L'utilisation actuelle de ces implants devra aussi être déterminée plus précisément afin de savoir dans quelles mesures la réalité rejoint aujourd'hui la fiction.

9 Ces outils de traçabilité posent de nombreuses difficultés eu égard au contexte juridique et éthique existant

aujourd'hui[3], notamment au regard de leur quasi invisibilité. Les grands principes fondamentaux actuels ne sont effectivement pas en adéquation avec ce type de technologie. Sur le plan interne, ils se heurtent aux principes généraux des législations nationales, tandis que sur le plan européen ou international, conventions, déclarations et chartes viennent limiter l'impact de ses puces sur les individus. Certains principes sont d'ailleurs récurrents et seront développés ultérieurement. Il s'agit entre autres, du respect de la dignité humaine ou de la protection de la vie privée et des données à caractère personnel. D'autres principes secondaires viennent les renforcer tel, par exemple, le principe de proportionnalité.

10 Les implants TIC, puces RFID sous-cutanées, sont confrontés, en sus de ceux déjà nommés, à d'autres principes fondamentaux plus spécifiques, tels l'inviolabilité de la personne humaine ou encore le principe de précaution qui prévoit la mise en place de mesures préventives avant toute action concrète, principe indispensable lorsqu'il s'agit d'opérations réalisées sur le corps humain.

11 En parallèle, les données éthiques vont également jouer un rôle très important. De nombreux principes sont fondés sur des raisons éthiques et vont ainsi empêcher le développement irraisonné des puces RFID. Il en est ainsi des principes de non discrimination ou de consentement éclairé qui complètent sinon empiètent sur les principes mis en place par les normes juridiques. Toutefois, il serait trop simple de limiter la question de cette technologie au respect de ces principes. Des conflits de valeurs existent qui pourraient remettre en cause l'application même de ces droits fondamentaux, notamment dans le cadre de l'utilisation des implants. La protection du plus grand nombre de personnes ne justifierait t'elle pas la limitation de la liberté d'individus jugés dangereux pour la société ?

12 Certaines législations françaises démontrent déjà qu'il est possible de venir limiter les libertés de certains individus afin d'assurer la sécurité publique. La loi Perben II en est

un exemple particulièrement concret. La loi Perben II du 9 avril 2004 a d'ailleurs fait l'objet d'une saisine du Conseil Constitutionnel en ce sens qu'elle violait la liberté individuelle garantit par l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789.

13 Quelles sont les utilisations actuelles et potentielles des puces RFID et des implants sous-cutanés ? Quels risques ces technologies font-elles encourir ? Dans quelles mesures les droits fondamentaux et les principes éthiques vont-ils circonscrire l'application de cette technologie ? Les valeurs défendues par la société sont-elles à même de supplanter ces libertés fondamentales ? Il conviendra d'étudier l'avancée de cette technologie (I), avant d'envisager le cadre juridique qui pourrait venir la circonscrire (II).

I - Le développement de technologies intrusives et invasives

14 Afin d'appréhender globalement les technologies relatives aux puces RFID et aux implants TIC, il apparaît nécessaire de connaître les utilisations actuelles et futures qui en seront faites (A) avant de s'intéresser aux obstacles pouvant ralentir leur irrésistible ascension (B).

A/ Les utilisations actuelles et potentielles

15 La puce RFID ne fait pas partie des technologies émergentes, néanmoins sa miniaturisation permet d'entrevoir une multitude de possibilités qui vont amener cette technologie à se généraliser. Avant d'entrevoir l'ensemble des possibilités qu'offrent ces puces, il apparaît judicieux d'en connaître plus précisément le fonctionnement.

16 Le principe de la technologie RFID repose sur deux éléments distincts, l'étiquette, appelée aussi radio tag ou transpondeur, et le lecteur qui possède une source autonome d'alimentation. L'étiquette est composée d'une puce électronique, comprenant l'unité de contrôle, la mémoire et l'alimentation, et d'une antenne bobinée ou

imprimée[4]. L'alimentation de la puce est assurée par un « mécanisme de production d'énergie, par les réactions du bobinage de l'antenne à la traversée d'un champ électromagnétique, qui dispense de piles et assure un usage illimité »[5]. Ce champ électromagnétique est émis par le lecteur. Ce dernier peut être réparti en plusieurs catégories différenciées par la fréquence utilisée. Il existe ainsi quatre fréquences principales, choisies en fonction de l'utilisation qui va en être faite.

17 Les puces RFID sont aujourd'hui répandues dans de nombreux secteurs d'activités. La distribution est certainement le plus grand vecteur d'application de cette technologie. En premier lieu, la puce RFID vise à remplacer le code-barres, par le biais d'un système de standardisation. Cette standardisation est rendue possible grâce à l'*Electronic Product Code* (EPC) qui fournit pour chaque bien manufacturé, un numéro d'identification unique alors que les codes actuels permettent seulement de donner un numéro pour une classe de produits. Cette standardisation vise entre autre chose à lutter contre la contrefaçon. En effet, l'attribution d'un code unique à chaque objet permettrait de vérifier son authenticité. La technologie RFID est également utilisée pour la réalisation d'inventaires, notamment par la chaîne de magasins Walmart, et certaines entreprises utilisent déjà cette technologie pour mettre en place l'ensemble de leurs chaînes logistiques. Tel est le cas pour le transporteur allemand DHL et le distributeur Metro. Le but de cette opération est de pallier aux erreurs humaines mais également d'améliorer la traçabilité de l'ensemble des produits. Ainsi, quand une palette passe sous le portique, ce dernier scanne en masse les produits et vérifie si la palette est en partance pour la bonne destination. Dans un futur proche, il est envisageable que cette technologie permette de scanner automatiquement et sans contact l'intégralité d'un caddie. En pratique, chaque produit possédant une référence l'identifiant, ce numéro sera lu par un lecteur, transmis à un ordinateur qui interrogera

une base de données contenant l'ensemble des références EPC et identifiera l'objet. Néanmoins, Pierre Blanc, program manager pour le groupe Carrefour annonçait en 2008 que « les technologies RFID actuelles ne sont pas encore assez satisfaisantes pour pouvoir assurer une garantie à 100 % que tous les produits sont scannés lors du passage en caisse »[6]. L'hétérogénéité des produits en est la conséquence, certaines fréquences radio rendant impossible la lecture à travers les liquides par exemple. Dans un avenir proche, la technologie NFC (*Near Field Communication*) permettra à des objets dotés de puces sans contact de communiquer entre eux. Elle permettrait par exemple de commander un produit en approchant une carte bleue, dotée d'une radio-étiquette, d'une affiche publicitaire, elle aussi équipée d'une puce.

18 Faisant suite à la distribution, le secteur des transports voit lui aussi nombres d'intérêts à ces radio-étiquettes. Aux Etats-Unis, le *Speed Pass*, sorte de « porte-monnaie électronique sans fil » est aujourd'hui plébiscité par nombres d'utilisateurs et d'enseignes, notamment les stations-service et les chaînes de restauration rapide. Ce système original offre divers dispositifs de paiement tel un tag autocollant à apposer sur la lunette arrière d'un véhicule ou des microsémetteurs portatifs pouvant être inclus dans un porte-clés voire une montre. Des terminaux permettent l'identification de l'usager par le biais de la puce RFID lors d'une opération commerciale et, le cas échéant, le débit de son compte bancaire. En France, le STIF (Syndicat des Transports d'Île-de-France), autorité organisatrice des transports en région parisienne, a récemment opté pour cette technologie en créant le Pass Navigo, remplaçant de la Carte Orange et des traditionnels coupons à oblitérer. Ce choix est avant tout justifié par un souci de régulation des flux et de connaissance des usages. Dorénavant, pour accéder aux réseaux RATP ou RER, l'usager francilien n'a qu'à apposer son Pass contre un lecteur incorporé à la borne d'accès pour qu'un terminal détermine la validité de l'abonnement puis permette le

passage.

19 Le secteur de la santé semble lui aussi être concerné par la mise en place des puces RFID, toutefois le projet n'a pas encore traversé l'Atlantique. En effet, la *Food and Drug Administration*[7] a envisagé un programme de lutte contre la contrefaçon de médicaments en apposant des puces dans les emballages.

20 De même, en apportant de façon instantanée des informations multiples et complexes, la RFID pourrait devenir un important vecteur en matière de protection environnementale, notamment en matière de gestion des déchets et des ordures ménagères. A plus grande échelle, la technologie RFID pourrait, dans un futur proche, permettre de réguler le gaspillage des ressources naturelles. Des systèmes associant tags RFID et capteurs hygrométriques permettent déjà de déterminer les besoins de parcelles agricoles en irrigation et optimisent l'arrosage des cultures, évitant ainsi les ponctions excessives au milieu aquifère.

21 Concernant le domaine de la sécurité, les applications de la radio-identification revêtent maints aspects. La Banque Centrale Européenne songe par exemple, dans la lutte contre le faux-monnayage, à sécuriser les billets d'Euro en leur enjoignant une nano-puce dont l'épaisseur ne dépasserait pas quatre millimètres. Certaines maternités canadiennes dotent leurs nouveau-nés de bracelets électroniques pour prévenir les situations à risques tels de potentiels enlèvements. Ces bracelets sont équipés d'émetteurs reliés à un ordinateur central, les récepteurs répartis dans la maternité permettent de localiser le bébé à tout moment et de détecter les éventuelles sorties du service. ADP (Aéroports de Paris) développe les technologies RFID autant pour la gestion des bagages transitant sur ses plates-formes que pour l'accès aux zones réservées et sécurisées. La technologie RFID a également été installée dans les badges afin de contrôler l'accès à des bâtiments sensibles ou à certains congrès. Ainsi au dernier congrès du Parti Communiste chinois, les invités étaient

munis d'un badge, renvoyant à un index sur une base centrale et présentant la photo du titulaire au service de sécurité. De même, lors du Sommet mondial de la Société de l'Information organisé à Genève en 2003, il fut révélé, postérieurement à la Conférence, que les badges qui avaient été remis aux participants étaient dotés d'une puce RFID contenant entre autres, le nom, la photo, la fonction et l'organisation de rattachement de chaque invité.

22 Le Conseil Européen s'est engagé quant à lui à doter les passeports des États membres de la technologie RFID par l'utilisation d'une puce stockant les données biométriques du porteur comme sa photographie numérisée, son état civil ainsi que deux empreintes digitales[8]. Par un décret du 30 avril 2005, le gouvernement français a mis en place le passeport électronique dit DELPHINE (DELivrance de Passeports à Haute-INtégriT de sécuritE) composé d'une zone de lecture optique et d'une puce RFID contenant des données administratives et physiques sur son détenteur Le 28 juin 2009, le passeport biométrique a remplacé le passeport électronique sur tout le territoire français.

23 Les radios marqueurs sous-cutanés sont utilisés dans un premier temps pour assurer la traçabilité des animaux de compagnie ou celle du bétail. Applied Digital Solution est la première société à proposer la puce Verichip destinée aux humains. L'implant sous-cutané se présente sous la forme d'un tube en verre ultra-résistant de la taille d'un grain de riz contenant une puce électronique, un émetteur, un récepteur et une antenne.

24 L'implant TIC propose deux types d'applications majeures que sont le stockage de données et la surveillance de l'individu. L'agence de sécurité sanitaire américaine a autorisé, en octobre 2004, l'usage des puces RFID dans le corps humain, à des fins médicales. Les puces sont injectées dans le bras des patients à l'aide d'une seringue. Pour des raisons de confidentialité, le dossier médical du patient n'est pas contenu dans la puce proprement dite. Le personnel médical doit utiliser un scanner qui identifie un numéro de série unique et donne accès aux informations

présentes dans une base de données distante. En 2006, 78 hôpitaux avaient accepté de participer à des projets pilotes aux Etats-Unis et de nombreux patients s'étaient fait implanter afin que les services d'urgences puissent les identifier rapidement en cas d'accident et aient accès à leurs dossiers médicaux. Une application plus marginale du stockage de données est en train de se développer. L'exemple le plus frappant est certainement celui du Baja Beach Club situé à Barcelone. Cette discothèque a offert à ses clients VIP la possibilité de se faire implanter un dispositif RFID sous la peau. Cette puce contient le nom, la photo et le numéro matricule du client. Pour payer ses consommations, ce dernier approche son bras d'un scanner qui affiche l'état du compte qu'il a ouvert et qui sera débité automatiquement.

25 Les implants TIC trouvent d'autres applications telles la surveillance ou encore l'authentification. Au Mexique, le ministre de la Justice et deux cent de ses collaborateurs se sont fait injecter une puce sous-cutanée afin de contrôler l'accès aux zones sensibles où des documents confidentiels sont conservés. Les autorités de ce pays attendent également l'arrivée de scanners plus puissants afin de contrôler les allées et venues des fonctionnaires[9]. Ce mode de surveillance des individus avait pour dessein originaire la traçabilité des personnes atteintes de la maladie d'Alzheimer et des jeunes enfants en cas de kidnapping. La justice anglaise a souhaité élargir son champ d'application en implantant des puces sous la peau des délinquants. Ce projet n'a toutefois pas vu le jour en raison de problèmes techniques. En effet, pour communiquer, la puce a besoin d'un complément externe. Les volontaires auraient dû rester près d'un lecteur, car la puce ne permet de suivre les déplacements qu'à proximité d'un scanner. Pour le moment, la puce Verichip n'est donc pas un système implantable de positionnement par satellite[10]. Cependant des recherches sont en cours visant à créer un système sous-cutané de positionnement par satellite qui permettrait effectivement de localiser et d'identifier

partout dans le monde des enfants enlevés ou encore des terroristes présumés. La société ADS prévoit également pour l'avenir, la mise en place d'armes intelligentes qui ne peuvent tirer que si elles sont actionnées par leur propriétaire auquel serait implantée une puce RFID dans la main.

26 Au vue des applications existantes et de celles à venir, la technologie RFID semble être en phase de se généraliser. Cependant des problèmes techniques existent, qu'il serait judicieux de régler avant tout autre chose.

B/ Les limites techniques de ces formes de surveillance et d'intrusion

27 Les applications reconnues aux puces RFID sont nombreuses, il n'en reste pas moins que ces dernières présentes un certain nombre de lacunes. Certaines font obstacles à leur pleine et entière application tandis que d'autres remettent en cause leurs utilisations proprement dites.

28 Trois obstacles majeurs freinent le développement des puces RFID. La première limite technique est relative aux fréquences des lecteurs. Il apparaît que certaines fréquences rendent difficiles la lecture à travers les liquides[11] – donc le corps humain, tandis que d'autres sont sensibles aux perturbations radio[12]. Ces lacunes nuisent à la généralisation de cette technologie et c'est pourquoi le fait de scanner un caddie entier de produits de consommation ne peut, à ce jour, être mis en œuvre. L'obstacle suivant vaut pour l'ensemble des puces RFID. La lecture de radio-étiquettes apposées sur des objets contenus dans un environnement métallique tel un conteneur, est très difficile et la distance de communication possible est fortement réduite. La dernière limite technique recensée est celle de la collision. Lorsque plusieurs marqueurs se trouvent dans le champ d'un même lecteur, les communications se trouvent brouillées par l'activité simultanée de ces derniers. Afin de pallier à cet inconvénient, plusieurs méthodes d'anticollision ont

été développées dont les principales sont les méthodes fréquentielles, spatiales, temporelles et systématiques. Ces dispositifs n'apportent cependant pas une solution parfaite au problème. La méthode fréquentielle consiste à faire communiquer chaque marqueur sur une plage de fréquence différente avec le lecteur. Cette méthode s'avère impossible à mettre en œuvre à grande échelle. La méthode spatiale fonctionne avec l'aide d'une antenne directionnelle qui va permettre au lecteur de couvrir chaque partie de l'espace pour communiquer avec chaque marqueur. En pratique, la proximité entre deux puces RFID rend la méthode inapplicable. Le système temporel s'appuie sur des canaux de temps. Le lecteur va proposer différentes plages et chaque marqueur en choisira une de manière aléatoire. La méthode sera renouvelée jusqu'à ce que tous les marqueurs aient choisi une plage de temps différente. Ici, le côté aléatoire rend la durée de lecture absolument inconnue. Enfin la dernière méthode paraît certainement la plus efficace même si sa durée reste longue. Elle consiste à détecter puis à enregistrer tout à tour l'ensemble des marqueurs en parcourant l'arbre de toutes les possibilités d'identifiants.

29 Un écueil supplémentaire concerne plus particulièrement les puces RFID sous-cutanées. En effet, les risques sanitaires inhérents aux implants TIC ont été soulignés par la *Food and Drug Administration* dans une ordonnance concernant la puce sous-cutanée Verichip. Cette ordonnance fait état de plusieurs menaces potentielles pour la santé telle une réaction tissulaire, la migration du transpondeur implanté, des perturbations électromagnétiques ou encore des risques électriques[13]. De même, dans un rapport du 26 janvier 2009, l'AFSSET[14] recommande de poursuivre les études scientifiques sur la recherche d'effets biologiques liés aux rayonnements des puces RFID. En effet, des études américaines avaient démontré une augmentation de 10 % des cancers liés au RFID chez les rats.

30 Le piratage des puces RFID remet en cause l'utilisation

même de cette technologie. De nombreuses études démontrent que les puces RFID actuelles peuvent être piratées voire clonées. En juillet 2006, un groupe de hackers annonçaient à la convention biannuelle Sixth Hope à New York, avoir cassé les sécurités de la puce sous-cutanée. En novembre 2006, le New York Times publiait les résultats d'une étude universitaire portant sur la première génération de cartes de crédit dotées de puces RFID. Lancées en 2005, elles sont d'ores et déjà utilisées par 20 000 000 d'américains et plus de 150 000 magasins. Selon cette étude « aucune des vingt types de cartes qu'ils ont testées n'a résisté à leurs attaques, et toutes faisaient fuiter les noms, numéros de carte, dates de validité et autres données contenues dans les puces, de sorte qu'il est possible de les cloner sans grande difficulté »[15]. Adam Laurie, un chercheur britannique spécialisé dans les systèmes de sécurité a, lors de la ShmooCon Convention de Washington, piraté la puce RFID qu'un membre de l'assistance s'était fait poser sous la peau. En 2009, il ne mettra que douze minutes pour pirater la nouvelle carte d'identité britannique équipée de la technologie RFID. Le procédé dont il a usé est le suivant : Adam Laurie a tout d'abord cracké l'algorithme de sécurité de la puce, puis il a copié toutes les données qu'elle contenait avant de cloner la carte d'identité. Il est à noter que le chercheur a également pu modifier l'ensemble des données de la carte clonée.

31 Antérieurement à cette prouesse, mais fort des piratages déjà réalisés, le département de la sécurité intérieure des États-Unis avait d'ailleurs rendu un rapport sur l'utilisation de la RFID pour l'identification humaine et déconseillait cette application qui aurait « plutôt tendance à accroître les risques en matière de sécurité et de protection des données personnelles, sans avantage commensurable en termes de performances ou de sécurité nationale »[16]. Cependant, il apparaît que le danger n'est pas limité aux implants sous-cutanés, le passeport biométrique livrant par exemple lui aussi énormément

d'informations relatives à la vie privée des personnes.

32 Le piratage étant possible, il est vite apparu que les puces étaient également vulnérables aux virus. Spécialiste du sujet, le professeur Andrew S. Tanenbaum membre de l'Université d'Amsterdam, a démontré qu'en exploitant une faille du système RFID, on pouvait introduire un virus et atteindre ainsi la base de données. Il démontre par un exemple concret que cela pourrait s'avérer désastreux. Une étiquette ainsi modifiée pourrait être accolée volontairement sur un produit de consommation à l'intérieur d'un magasin. Lors du passage en caisse, le produit ainsi scanné pourrait infecter toute la base de données du magasin, en changeant tous les prix par exemple.

33 Des solutions sont envisagées pour empêcher le piratage, telle la cryptographie. Néanmoins, il y a fort à penser que les hackers auraient tôt fait de mettre à mal cette protection.

34 Outre les limites techniques, les droits fondamentaux et les principes éthiques viennent également freiner le développement de ces technologies intrusives. Il est donc nécessaire de leur fournir un cadre normatif limitant leurs impacts sur les libertés.

II - La nécessaire normalisation de ces outils de traçabilité

35 Ces outils de traçabilité ont besoin d'un cadre normatif pour se développer. La puce RFID existe depuis longtemps, mais les nombreuses avancées en ce domaine, dont la miniaturisation, induisent une législation renforcée au même titre que les implants TIC. Cette réglementation doit s'accommoder des différentes libertés fondamentales qui s'opposent à ces technologies (A), tout en sachant les contourner lorsque l'intérêt plus grand se présente (B).

A/ Un développement freiné par les droits fondamentaux et les principes éthiques

36 La CNIL s'est intéressée au rapport existant entre la technologie RFID et les éventuelles atteintes aux droits fondamentaux et plus particulièrement au respect de la vie privée et des données à caractère personnel. Il ressort de cette réflexion que la généralisation des puces RFID porte atteinte à ce droit défendu par l'article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme et du Citoyen[17], et ce même si « quatre pièges peuvent masquer l'importance cruciale des enjeux « Informatique et Libertés » de cette technologie »[18]. Le premier piège est relatif à l'insignifiance des données. Nul ne s'inquiète du fait que sa boîte de petits pois possède un numéro de série l'identifiant. Cependant, le problème provient de la multiplicité du volume d'information qui, par le biais d'un maillage très dense, permet le profilage des individus. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a pris en compte cette possibilité lors de sa modification donnant lieu à la loi du 6 août 2004. Elle introduit dans son article 2 définissant les données à caractère personnel, une nouvelle catégorie, celle des informations permettant d'identifier un individu. Cette loi reconnaît la possibilité que la multiplication et le recoupement d'informations puissent conduire à identifier des personnes. En effet, la présence dans l'avenir d'un identifiant unique pour chaque objet manufacturé, permet par exemple, par simple lecture des tags qu'une personne porte sur elle à l'entrée d'un magasin, de connaître ses habitudes de consommation. De même, sans connaître l'identité d'une personne, celle-ci peut être identifiée par le biais des objets qui l'entourent. Ainsi, « il serait alors possible de savoir que quelqu'un ayant sur lui le manteau dont le numéro est XXXX était dans le secteur où un larcin a été commis, il suffira de rechercher le manteau (ou une combinaison d'objets si l'on veut une preuve plus sûre) qui répond à cet identifiant pour retrouver le suspect »[19]. L'atteinte à la vie privée est donc ici non négligeable.

37 Le second piège est celui de la priorité donnée aux objets dans l'application de cette technologie, ce qui contribue à

endormir la vigilance. Philippe Lemoine fait également état d'une logique de mondialisation qui établit les standards de ces puces au regard des enjeux économiques dictés principalement par les sponsors américains, ce qui vise, comme nous le verrons ultérieurement, à favoriser cette technologie aux dépens des droits fondamentaux. La non-vigilance individuelle est le dernier faux-semblant que dévoile la CNIL. Avec les puces RFID, les données sont saisies à distance, sans que le porteur en soit averti. Pour Michel Alberganti, « le caractère involontaire de la fourniture d'informations personnelles »[20] est la caractéristique la plus importante en terme de menace pour les libertés individuelles puisqu'aucune autorisation, aucun geste n'est demandé pour activer les puces. Ces « quatre pièges » tendent effectivement à minimiser l'impact des puces RFID sur la vie privée. Cependant l'atteinte existe bel et bien et la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 va tenter d'en amoindrir les effets.

38 Les implants TIC sont également confrontés au principe du respect de la vie privée. Les puces sous-cutanées peuvent contenir des données à caractère personnel, tel le dossier médical du patient et leurs confidentialités doivent être respectées. Toute personne doit pouvoir déterminer quelles données le concernant peuvent être traitées et à quelle fin. Ce droit fondamental – qui est également un principe éthique – est d'autant plus important lorsque les implants fonctionnent en ligne notamment dans le cadre de dispositif de surveillance.

39 Cependant, au regard de cette technologie, le respect de la vie privée est loin d'être le seul principe à faire barrage au développement de ce type de puces. L'ensemble de ces principes dessineront en grande partie le cadre juridique qui circonscrira l'utilisation des implants TIC[21] et éviteront tout débordement.

40 La Charte des droits fondamentaux de l'Union Européenne expose dans son article premier que « la dignité humaine est inviolable. » Ce principe est consacré dans l'arrêt

Omega[22] de 2004 dans lequel la Cour de justice juge légale l'interdiction par les autorités allemandes du jeu « Jouer à tuer », considéré comme portant atteinte à une valeur fondamentale, « à savoir la dignité humaine. » L'importance de ce principe est telle que dans certains cas, le consentement éclairé de la personne s'avère insuffisant pour faire de certaines technologies un objet légalement acceptable. Certaines atteintes au corps humain seront alors interdites au regard de la dignité humaine et ce afin que les transformations subies par ce dernier ne fasse pas de lui un objet pouvant être manœuvré et surveillé à distance.

41 Le principe d'inviolabilité du corps humain est énoncé à l'article 3 de la Charte des droits fondamentaux et exclut tout activité susceptible de compromettre son intégrité et ce, malgré le consentement de la personne concernée. De surcroît, nombres de réglementations, dont l'article 21 de la Convention sur les droits de l'homme et la biomédecine et l'article 4 de la Déclaration universelle de l'Unesco, limitent la liberté d'user de son corps et interdisent donc de faire du corps humain une source de profit. Le groupe européen d'éthique semble penser qu'une interprétation plus large de ce principe de non-commercialisation pourrait mener à penser que l'implantation de dispositifs TIC à des fins mercantiles ne soit pas autorisée. Ainsi, l'implantation de puces Verichip dans le but d'accéder à une discothèque serait prohibée.

42 Les puces RFID sous-cutanées vont être confrontées au principe de précaution au sein de l'Union Européenne. Malgré le fait que ce principe ne soit prescrit qu'une seule fois dans le Traité pour les questions ayant trait à l'environnement, la Commission Européenne, dans une communication de février 2000 estime que « son champ d'application est beaucoup plus vaste, plus particulièrement lorsqu'une évaluation scientifique objective et préliminaire indique qu'il est raisonnable de craindre que les effets potentiellement dangereux pour l'environnement ou la santé humaine, animale ou végétale

soient incompatibles avec le niveau élevé de protection choisi pour la Communauté. » Les conditions nécessaires à l'application du principe de précaution sont l'existence d'un risque, la possibilité d'un dommage et une incertitude concernant la survenance de ce dommage. Les mesures qui sont alors mises en œuvre pour garantir ce principe déterminent le niveau de risques acceptables au regard des valeurs en jeu. Il est incontestable que le respect du corps humain est l'une des valeurs qui appellent le plus haut degré de protection juridique. En ce sens, il y a fort à penser que les États membres de l'Union Européenne auront une démarche plus protectrice que les États-Unis. En effet, la *Food and Drug Administration* a autorisé les tests en vu d'un usage médical après avoir pourtant constaté un nombre conséquent de risques telles des réactions tissulaires, la migration du transpondeur ou encore des perturbations électromagnétiques.

43 Enfin, un certain nombre de principes ne concerne pas la légalité de l'implantation en elle-même mais s'intéressent plus particulièrement aux modalités de l'utilisation des implants TIC. Ce sont les principes de minimisation des données, de spécification de la finalité, de proportionnalité et de pertinence. L'article 16 paragraphe 2 du Code civil français dispose « (qu') il ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité pour la personne. » Cela signifie que l'on ne peut recourir à cette éventualité que si le but poursuivi ne peut être atteint par d'autres moyens moins contraignants Le principe de minimisation ici mis en œuvre signifie que la légitimité ne saurait être accordée à des implants ayant pour seule finalité l'identification des individus, s'il s'avère que d'autres moyens moins invasifs peuvent être mis en œuvre. Le principe de spécification des données suppose de sélectionner les objectifs à atteindre. Les implants TIC à visée médicale paraissent plus en adéquation avec ce principe, cependant les applications médicales devront elles aussi être évaluées afin d'éviter d'éventuels détournements de finalités. Le principe de

proportionnalité concerne plus particulièrement l'instrument qui sera utilisé pour atteindre l'objectif. En d'autres termes, même si l'objectif est jugé légitime, il ne pourra être poursuivi par le recours à un instrument disproportionné. Le principe de pertinence prévu à l'article 6 de la directive 95/46/CE[23] impose un rapport étroit entre la technologie utilisée et la situation traitée, afin d'éviter tout abus.

44 Les quatre principes précités se complètent, car une fois démontrée l'existence d'un objectif légitime justifiant l'utilisation des implants TIC, il faudra démontrer que ce dernier est nécessaire, proportionné au but à atteindre et pertinent.

45 L'ensemble de ces principes remet en cause la légalité de nombreuses utilisations existantes ou envisagées des puces sous-cutanées. Ce sont les implants TIC utilisés à des fins de surveillance qui posent les plus de problèmes. Le Groupe Européen d'éthique insiste sur le fait que ces implants ne sauraient être autorisés que si le législateur « estime que la société démocratique en a un besoin urgent et justifié et qu'il n'existe pas de méthode moins intrusive »[24]. Il insiste également sur la nécessité d'une réglementation afin d'assurer notamment le respect de la vie privée et des données à caractère personnel.

46 Il apparaît évident que ces principes contenus pour la plupart dans la Charte des droits fondamentaux de l'Union Européenne vont servir de base à une législation moderne concernant les nanotechnologies. Cependant, d'autres considérations semblent venir les concurrencer, permettant la mise en place d'une réglementation privilégiant d'autres valeurs que celles reconnues par les principes fondamentaux suscités.

B/ La possibilité d'une législation s'émancipant de ces principes

47 Les technologies de radio-identification sont susceptibles de permettre l'identification des personnes et, à ce titre, plusieurs législations peuvent leur être applicables. En

France, au premier plan de ces textes figurent la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et nommée aujourd'hui loi 2004/801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. La CNIL est une autorité administrative indépendante instituée par cette loi et en charge de veiller à la protection de ces données.

48 La loi de 1978 impose des obligations aux responsables mettant en œuvre les fichiers nominatifs et, dans un même temps, octroie un certain nombre de droits aux personnes physiques en ce qui concerne le traitement de leurs données personnelles.

49 La réglementation a ainsi instauré plusieurs limites à la constitution de fichiers nominatifs. En premier lieu, les responsables des fichiers sont soumis à l'obligation de loyauté et d'information. Ils doivent signifier aux individus la collecte d'information les concernant et certaines données sensibles commandent l'accord express des individus. L'article 6 qui régit ce principe dispose d'un pendant pénal qui punit de cinq ans d'emprisonnement et de 300 000 € d'amende, le non-respect de cette obligation. Le principe de finalité est également entendu même s'il n'est pas clairement défini dans la loi. Ce principe rappelle que les données collectées pour certaines finalités ne devront pas être détournées de leur objectif initial lorsqu'elles seront traitées. Enfin, la législation, dans son article 34, impose une obligation de sécurité et de confidentialité des données.

50 Les personnes physiques possèdent également des droits en ce qui concerne le traitement de leurs données. Le droit d'accès assure à toute personne justifiant de son identité, le droit d'interroger le responsable du fichier afin de savoir si des informations la concernant sont traitées[25]. Ce droit est payant et la loi de 2004 rappelle que le prix à débourser ne doit pas « excéder le coût de la reproduction. » Devant la généralisation assurée de cette technologie, le droit d'accès de l'individu semble être remis en cause.

Techniquement, il est fort improbable qu'une personne puisse contrôler l'ensemble des données la concernant qui seront traitées. Le droit de rectification, qui est le corollaire du droit d'accès, risque de voir son efficacité réduire d'autant. L'article 38 de cette même loi met en place un droit d'opposition au traitement des informations. Là encore, outre le fait qu'un certain nombre de traitements imposés par l'État ne seront pas susceptibles de se voir opposer ce droit (passeports, billets de banque), la généralisation et l'invisibilité de cette technologie rendront très difficile un contrôle a posteriori. Il y a fort à penser que la loi devra s'adapter à ces nouvelles contraintes afin d'assurer un meilleur respect de la vie privée.

51 Une autre réglementation, concernant la possibilité de désactivation des tags, peut être envisagée dans l'utilisation de la radio-identification. En effet, en matière de données personnelles, deux grands principes coexistent et sont désignés sous les anglicismes d'OPT OUT et d'OPT IN. Le premier présume que la personne dont les données personnelles sont collectées a donné son accord tandis que le second suppose que tout individu qui n'a pas donné expressément son accord est opposé à la collecte de données le concernant.

52 Selon la CNIL, le meilleur moyen d'assurer la protection de la vie privée serait de désactiver les tags RFID dès la sortie des magasins « dans certaines situations et avec le libre choix des personnes »[26]. Cette solution semble se rapprocher de la notion d'OPT OUT et la désactivation n'est donc effective que si la personne concernée le demande expressément. En parallèle, les tendances européennes en ce domaine semblent écarter ce principe antérieurement usité[27]. La directive 2002-58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, met en œuvre le principe de l'OPT-IN et montre une volonté de renforcer la protection des citoyens européens. Une recommandation

de la Commission européenne du 12 mai 2009, sur la mise en œuvre des principes de protection de la vie privée et des données personnelles dans les applications fondées sur la RFID, est venue confirmer cette solution en précisant que lorsqu'un produit est équipé d'une puce RFID, celle-ci devra être désactivée automatiquement, immédiatement et gratuitement dans le magasin sauf si le consommateur demande expressément le maintien de la puce active[28].

53 De nombreux obstacles, tant pratiques que juridiques viennent nuancer cette obligation et passer outre le principe du respect de la vie privée et des données à caractère personnel. Les tags RFID utilisés par les autorités publiques, tels les passeports biométriques ou encore les billets de banque, ne pourront être désactivés sous peine de s'exposer à une sanction. Dans cette optique, l'État concerné devra s'assurer que les informations contenues dans la puce ne puissent être lues que par les autorités compétentes, ce qui au vu des récents piratages paraît pour le moins incertain. Un second problème résidera dans le fait que toute autorité compétente pourra contrôler un individu à son insu et sans motif particulier. La désactivation des puces RFID sera également impossible dans le cadre de l'exercice d'un droit. En effet, si la puce RFID s'avère nécessaire à l'accomplissement d'une prestation comme l'accès aux transports publics ou aux péages routiers, la désactiver reviendrait à priver l'utilisateur du service offert.

54 La recommandation du 12 mai 2009 envisage toutefois certaines obligations pour les entreprises et les pouvoirs publics. Ainsi, ces derniers sont invités à informer clairement les consommateurs sur les données qui seront recueillies et la Commission préconise en outre un étiquetage clair permettant d'identifier les dispositifs RFID.

55 Toutefois, le principe d'OPT IN ne peut donc réellement s'appliquer qu'aux biens de consommation, et là encore l'Union Européenne, par ses directives, vient limiter le principe qu'elle a elle-même imposé.

56 La directive 2001-29 du 22 mai 2001, relative à l'harmonisation de certains aspects du droit d'auteur, consacre dans son article 6 la mise en place de mesures techniques de protection. Il est entendu par mesures techniques, toute technologie qui « dans le cadre normal de son fonctionnement, est destinée à empêcher ou à limiter, en ce qui concerne les œuvres ou autres objets protégés, les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur. » L'implantation d'une puce RFID peut ici être considérée comme une mesure de protection, car grâce à l'attribution d'un code unique pour chaque objet, l'authenticité de ce dernier pourra être vérifiée et le piratage empêché. Dans ce cas, le fait de retirer la puce constituerait alors un délit de contrefaçon. Ces constatations mènent à penser que la désactivation est en passe de devenir une exception. La transposition de cette directive en droit français a eu lieu dans le courant de l'année 2006. Le texte a été adopté par l'Assemblée nationale et le Sénat le 30 juin 2006.

57 Une difficulté persiste cependant. Le fait d'empêcher une personne propriétaire d'un objet, de détruire la puce qui y est contenue, s'oppose au droit de propriété contenu dans l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen. Ce droit à valeur constitutionnelle ne connaît que quelques exceptions, toutes devant répondre à des impératifs supérieurs afin de justifier l'atteinte portée au droit de propriété. La question est alors de savoir si la propriété industrielle et la lutte contre le piratage prévalent sur ce droit. Une réglementation plus avancée concernant cette nanotechnologie permettra sans doute de répondre à cette interrogation. Néanmoins, il apparaît que la législation actuelle privilégie la politique de lutte contre le piratage au détriment du respect de la vie privée et des données à caractère personnel.

58 La législation sur les implants TIC étant encore actuellement inexistante, seules des hypothèses peuvent être formulées sur leurs éventuelles émancipations au regard des droits fondamentaux précités. Il ressort tout de

même de ces suppositions qu'un certain nombre de conflits de valeurs pourraient venir entraver l'édiction d'une réglementation encadrée uniquement par des principes défendant les libertés individuelles. Il est ainsi envisageable qu'un souci de compétitivité économique dans le cadre de l'Union européenne prenne le pas sur le respect de la dignité humaine ou encore sur le respect de la vie privée et des données à caractère personnel. Cette éventualité est d'ailleurs corroborée par une décision de la Commission européenne relative à la radio-identification[29]. En effet, afin de ne pas nuire au développement économique des acteurs européens de la RFID, la Commission a décidé dans un rapport de 2007, de ne pas réguler cette technologie. La Commission s'est appuyée sur une étude de la Deutsche Bank qui estimait qu'en prenant compte des valeurs ajoutées tels les logiciels et les services, « le marché européen pourrait passer de 500 millions d'euros en 2006 à plus de sept milliards d'ici dix ans. » Cette institution ne souhaite donc pas mettre en œuvre de réglementations spécifiques aux puces RFID actuellement même s'il est vrai que certaines applications à ce sujet ont été prises, mais dans le cadre plus large d'une directive concernant le traitement des données à caractère personnel et la protection de la vie privée.

59 Pareillement, le principe de dignité humaine revêt une telle importance, que le consentement éclairé des personnes ne suffira pas toujours à rendre légalement acceptable certaines pratiques. De ce fait, un conflit, entre la liberté de chaque individu de se faire implanter un dispositif et ce que la société jugera acceptable au regard des droits fondamentaux et des principes éthiques, verra certainement le jour.

60 Le dernier et non le moindre de ces conflits de valeurs risque de concerner la surveillance des personnes présentant un danger pour la société. En effet, afin d'assurer la sécurité du plus grand nombre, il pourrait être envisagé d'implanter des puces sous-cutanées aux « criminels. » Cette supposition est fondée sur l'évolution

de la législation française en matière pénale. La loi Perben II a fait l'objet à cet égard de nombreuses controverses puisque accusée de bafouer les libertés fondamentales. L'opposition avait d'ailleurs saisi le Conseil Constitutionnel, arguant du fait que de nombreuses dispositions de cette loi, dont le prolongement de la garde à vue[30], violait la liberté individuelle garantie par l'article 2 de la Déclaration de 1789[31]. Si cet argument a été rejeté par le Conseil, ce dernier précise néanmoins que ces dispositions sont « de nature à affecter gravement l'exercice des droits et libertés constitutionnellement protégés[32] » si l'autorité judiciaire n'exerçait pas pleinement sa mission de gardienne des libertés individuelles mise en place par l'article 66 de la Constitution. La garantie des libertés individuelles repose donc entièrement sur la vigilance de cette autorité. Cette loi a également légalisé les procédures d'infiltration permettant à un enquêteur de surveiller des personnes suspectées. L'ensemble de ces innovations démontre l'intérêt de l'État de s'affranchir quelque peu des libertés fondamentales afin d'assurer l'ordre public. Dans le prolongement de cette législation, il pourrait ainsi être envisagé l'utilisation des implants TIC comme moyen de surveillance et de localisation des délinquants. La réglementation privilégierait ainsi l'ordre public au détriment des libertés fondamentales.

61 L'ensemble de ces présomptions restent de l'ordre de la conjecture et seul l'avenir nous permettra de savoir quelle politique obtiendra la priorité.

Notes

1. RFID est le sigle de *Radio Frequency Identification.*

2. J.-F. Mattéi, « Traçabilité et responsabilité », *Traçabilité et responsabilité*, P. Pedrot (dir.), Economica, p. 35.

3. Rapport du Groupe Européen d'Ethique (GEE) sur les aspects éthiques des implants TIC dans le corps humain du 16 mars 2005.

4. E. Ercolani, « RFID et technologies sans contact », *L'informaticien*, n° 64, décembre 2008.

5. Ph. Lemoine, « Communication de M. Philippe Lemoine relative à la radio-identification », CNIL, 30 octobre 2003.

6. E. Ercolani, *op. cit.*

7. La *Food and Drug Administration* (FDA) est l'administration américaine des denrées alimentaires et des médicaments

8. Le règlement n° 2252/2004 du Conseil européen du 13 décembre 2004 établit « des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres ».

9. Y. Eudes, « Digital Boys », *Le Monde*, 11 avril 2006.

10. http://ec.europa.eu/european_group_ethics/docs/avis20_fr.pdf

11. La très haute fréquence du RFID soit 869,5MHz.

12. La basse fréquence (125KHz) et la bi-fréquence (125KHz-7MHz).

13. P. Le Guyader, *Les systèmes électroniques et informatiques de surveillance : Contrôle de la vie privée des personnes et des biens*, Hermès Science Publications, 2008.

14. Agence Française de Sécurité Sanitaire de l'Environnement et du Travail.

15. http://www.futura-sciences.com/fr/news/t/technologie-1/d/le-piratage-des-puces-rfid_9905/

16. http://www.internetactu.net/2006/06/06/du-piratage-des-puces-rfid-y-compris-sous-cutanees

17. Article 8 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance (...) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

18. Ph. Lemoine, *op. cit.*

19. http://www.juriscom.net/documents/priv20041022.pdf

20. M. Aberganti et P. Georget, *La RFID : Quelles menaces, quelles opportunités ?*, Prométhée, 2008.

21. http://ec.europa.eu/european_group_ethics/docs/avis20_fr.pdf

22. CJCE, 12 octobre 2004, C-36/02, Omega/Oberbürgermaister Rec. P 19609.

23. Directive 95/46/CE du Parlement Européen et du Conseil du 24

octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

24. http://ec.europa.eu/european_group_ethics/docs/avis20_fr.pdf

25. Article 39 de la loi du 6 janvier 1978.

26. Ph. Lemoine, *op. cit.*

27. Les directives 97-66 (concernant la prospection par certains moyens de télécommunication) et 2000-31 (relative au commerce électronique et touchant à la prospection par voie d'e-mailing) ont opté pour une solution qui pose le principe de l'OPT OUT.

28. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

29. P. Le Guyader, *op. cit.*

30. Article 706-88 du Code de procédure pénale : la garde a vue pourra passer de 48 heures à 96 heures.

31. Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression.

32. Décision n° 2004-492 DC du 2 mars 2004 du Conseil constitutionnel.

Auteur

Anne-Lise Madinier

Référence électronique du chapitre

MADINIER, Anne-Lise. *La surveillance de demain : puces RFID et implants sous-cutanés* In : *Un monde sous surveillance ?* [en ligne]. Perpignan : Presses universitaires de Perpignan, 2011 (généré le 24 décembre 2019). Disponible sur Internet : <http://books.openedition.org/pupvd/3969>. ISBN : 9782354122942. DOI : 10.4000/books.pupvd.3969.

Référence électronique du livre

LABROT, Émilie (dir.) ; SÉGUR, Philippe (dir.). *Un monde sous surveillance ?* Nouvelle édition [en ligne]. Perpignan : Presses universitaires de Perpignan, 2011 (généré le 24 décembre 2019). Disponible sur Internet : <http://books.openedition.org/pupvd/3947>.

ISBN : 9782354122942. DOI : 10.4000/books.pupvd.3947.
Compatible avec Zotero