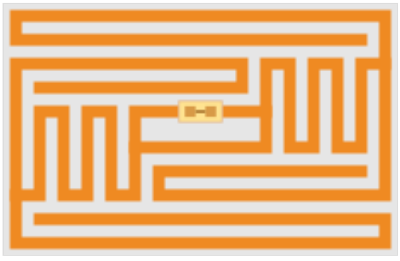
WIKIPÉDIA

Radio-identification

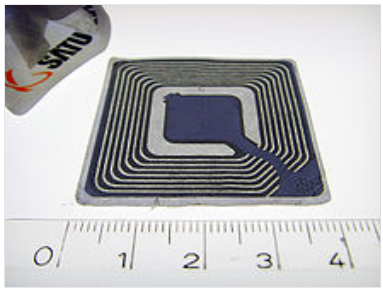
La **radio-identification**, le plus souvent désignée par l'acronyme **RFID** (de l'anglais « *radio frequency identification* »), est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« *RFID tag* » ou « *RFID transponder* » en anglais)[1].



Une puce de radio-identification EPC utilisée par Wal-Mart.

Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui sont collés ou incorporés dans des objets ou produits, et même implantés dans des organismes vivants (animaux, corps humain[2]). Les radio-étiquettes comprennent une antenne associée à une puce électronique qui reçoit et répond aux requêtes radio émises par l'émetteur-récepteur.

Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.

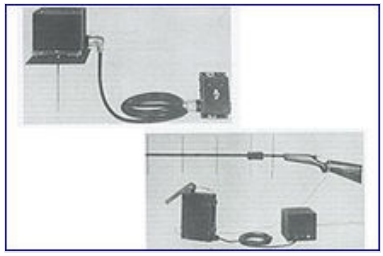


Cette technologie d'identification peut être utilisée pour identifier :

- les objets, comme avec un code-barres (on parle alors d'étiquette électronique) ;
- les personnes, en étant intégrée dans les passeports, cartes de transport, cartes de paiement (on parle alors de carte sans contact) ;
- les carnivores domestiques (chats, chiens et furets) dont l'identification RFID est obligatoire dans de nombreux pays, en étant implantée sous la peau. C'est également le cas de manière non obligatoire pour d'autres animaux de travail, de compagnie ou d'élevage commercial (on parle alors de puce sous-cutanée).

Historique

La première utilisation du RFID est militaire. Dès 1935, Robert Watson-Watt développe une application destinée à l'armée britannique, pour différencier les avions ennemis des alliés : c'est le système d'identification IFF « Identification friend or foe », qui reste le principe de base utilisé de nos jours pour le contrôle du trafic aérien[3].



IFF Modèle XAE, le premier système de reconnaissance IFF des États–Unis.

En 1945, Léon Theremin invente un dispositif d'espionnage pour l'Union soviétique, appelé « the thing », qui retransmet les ondes radio incidentes augmenté de l'information audio. Ainsi, ce dispositif assure la fonction d'un microphone sans fil transmettant un signal acoustique sur une onde porteuse RF. Les ondes sonores font vibrer un diaphragme qui modifie légèrement la forme du résonateur, lequel module la fréquence radio réfléchie. Même si ce dispositif est plus un dispositif d'écoute secrète qu'une étiquette d'identification, il est considéré comme un prédécesseur de la RFID parce qu'il est passif, car alimenté et activé par des ondes provenant d'une source extérieure[4].

Entre 1948 et 1952, H. Stockman et F. L. Vernon écrivent les premiers articles scientifiques sur la RFID[5,6]. Ces articles sont considérés comme les fondements de la technologie RFID[7]. Harry Stockman a notamment prédit qu' « ...un travail de développement et de recherche considérable doit être fait avant que les problèmes fondamentaux de la communication par puissance réfléchie soient résolus et que le domaine des applications utiles soit exploré... »[8].

Les années 1950 voient le dépôt de plusieurs brevets sur la RFID. En 1952 Donald Harris dépose le premier brevet d'un système de transmission communiquant avec une cible passive[9,10]. En 1959, J. Vogelman brevète un système communiquant avec une cible qui module le signal radar à travers la variation de la surface équivalente radar d'une antenne (SER)[11,12].

Dans les années 1960, les applications ont des buts commerciaux. Le premier tag fait son apparition en 1966. Cette première étiquette RFID (1-bit) est développée et commercialisée sous l'acronyme EAS (Electronic Article Surveillance), elle détecte uniquement la présence ou l'absence du tag. Le contrôle d'accès fait l'objet d'autres brevets[13,14,15,16]. La théorie fondamentale sur laquelle s'appuie la RFID est décrite dans plusieurs publications, dont celles de R. Harrington[17] et de J. K. Schindler[18].

« the thing », dispositif précurseur de la technologie RFID, caché dans un sceau.

Le dispositif de Mario Cardullo et William Parks, breveté le 23 janvier 1973[19,20], est le véritable ancêtre de la RFID moderne[21]. Il s'agit en effet d'un transpondeur radio passif, alimenté par le signal d'interrogation, et disposant d'une mémoire de 16 bits[20]. Il a été présenté en 1971 à la New York Port Authority et à d'autres utilisateurs éventuels. Le brevet de Cardullo couvre l'utilisation de la radiofréquence, du son et de la lumière comme supports de transmission. L'argumentaire commercial original présenté aux investisseurs en 1969 montre des utilisations dans les domaines des transports (identification des véhicules automobiles, péage automatique, plaque d'immatriculation électronique, manifeste électronique, routage des véhicules, suivi des performances des véhicules), de la banque (chéquier et carte de crédit électroniques), de la sécurité (identification du personnel, portes automatiques, surveillance), et de la santé (identification, antécédents du patient)[22,23].

Steven Depp, Alfred Koelle et Robert Frayman font une démonstration des étiquettes RFID à puissance réfléchie (rétrodiffusion modulée), à la fois passives et semi-passives, au Laboratoire national de Los Alamos en 1973[24]. Ils établissent l'expression reliant la puissance réfléchie à la charge de l'antenne, ce qui établit d'un point de vue formel le principe de la modulation du signal rétrodiffusé (ou « modulated backscatter » en anglais) des tags RFID. Le système portatif opère à 915 MHz et utilise des étiquettes 12 bits. Cette technique est employée par la majorité des étiquettes RFID UHFID et micro-ondes d'aujourd'hui[25].

Le premier brevet associé à l'abréviation RFID est accordé à Charles Walton en 1983[26,27].

Les années 1990 marquent le début de la normalisation pour une interopérabilité des équipements RFID[24].

En 1999, des industriels créent le centre d'identification automatique (Auto-ID Center) au MIT avec l'objectif de standardiser la technologie RFID[28]. Ce centre est fermé en 2003 lorsque les travaux sur le code produit électronique (EPC) sont achevés, et les résultats sont transférés à la EPCglobal Inc. fondée par le Uniform Code Council (UCC) et EAN International, dénommés maintenant GS1 US et GS1.

Depuis 2005, les technologies RFID sont majoritairement utilisées dans les secteurs industriels (aéronautique, automobile, logistique, transport, santé, vie quotidienne, etc.). L'ISO (International Standard Organisation) a participé à la mise en place de normes tant techniques que pratiques, atteignant un haut degré d'interopérabilité voire d'interchangeabilité[29].

Principe

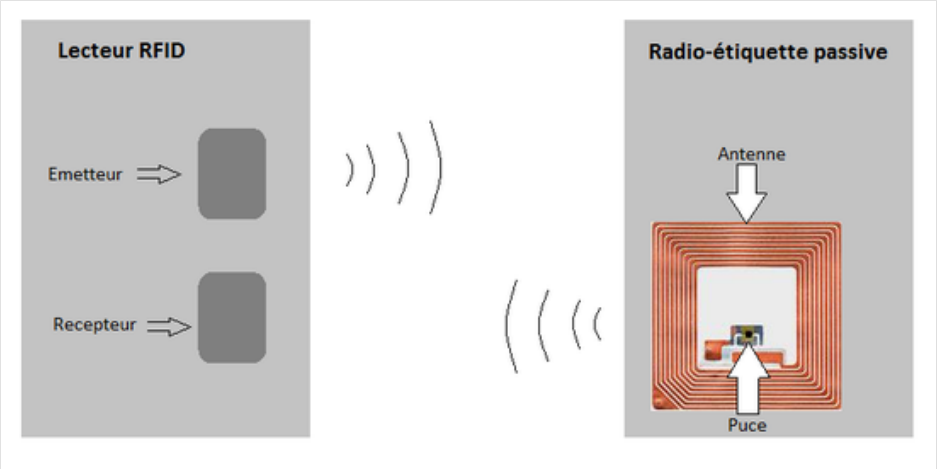
Un système de radio-identification est composé de deux entités qui communiquent entre elles :

- un marqueur, nommé radio-étiquette, tag RFID, ou encore transpondeur (de l'anglais *transponder*, contraction des mots *transmitter* et *responder*), apposé sur l'élément à identifier et encodant des données numériques ; les données sont lues sans ligne de vue directe, contrairement aux code-barres[30], avec une détection automatique et avec des distances de lecture supérieures (de 10 à 200 m selon le type de puces)[31].
- d'un ou plusieurs lecteurs RFID, appelés aussi interrogateurs, coupleurs, ou station de base[32].

À ces deux éléments s'ajoute généralement un intergiciel (middleware) ou application hôte, constitué d'un terminal (ordinateurs de supervision), connecté au lecteur, qui exploite les données collectées[33].

Le système est activé par un transfert d'énergie électromagnétique. Le lecteur agit généralement en maître, il envoie une onde électromagnétique en direction de l'objet à identifier. Il active ainsi le marqueur, qui lui renvoie de l'information[31].

Le lecteur envoie des requêtes aux tags RFID pour récupérer des données stockées dans leur mémoire. Le tag, généralement télé-alimenté par le signal du lecteur, génère en premier lieu un code identifiant l'objet sur lequel il est déposé. La communication entre les deux entités s'engage. Le lecteur procède à une écriture d'information dans le tag[34].



Principe de communication RFID avec une radio-étiquette passive

Lecteurs

Le lecteur est le composant qui coordonne la communication RFID et assure la télé-alimentation des tags dans le cas de la RFID passive. Il est composé d'un module radio fréquence pour la transmission et la réception, d'une unité de contrôle, d'une antenne, et d'une interface pour transmettre les données vers un terminal[35].

Les lecteurs sont des dispositifs actifs, émetteurs de radiofréquences qui activent les marqueurs qui passent devant eux en leur fournissant à courte distance l'énergie dont ceux-ci ont besoin. Ainsi, le lecteur est constitué d'un circuit qui émet une énergie électromagnétique à travers une antenne, et une énergie électronique, qui reçoit et décode les informations envoyées par les marqueurs, puis les envoie au dispositif de collecte des données[36]. Le lecteur est aussi à même d'écrire du contenu sur les tag RFID. Le lecteur RFID est l'élément responsable de la lecture des étiquettes radiofréquence, de l'écriture de contenu sur les tag RFID si besoin, et de la transmission des informations vers le middleware.

Fréquence

La fréquence établit la communication entre la puce et l'antenne. La fréquence varie en fonction du type d'application visé et les performances recherchées[37,38] :

- Basse fréquence
  - 125 kHz ;
  - 134,2 kHz pour la charge du transpondeur ; 134,2 kHz pour un bit 0, et 123,2 kHz pour un bit 1 pour la réponse du transpondeur dans le cas d'une transmission FSK (Texas Instruments Series 2000).

Les taille et poids réduits des tags sont idéaux pour être d'une part intégrés dans tout type de matériaux (textiles, métaux, plastiques, etc)[39], et d'autre part pour l'identification du bétail[37]. Grâce aux basses-fréquences la lecture se fait en tout milieu, mais à courte distance (quelques décimètres au maximum)[40].

- Haute fréquence
  - 13,56 MHz (ISO 14 443 A 1-4, ISO 14443B 1-4, ISO 15693-3 et ISO 18000-3), la plus répandue actuellement dans l'industrie et le grand public pour des applications à portée limitée.

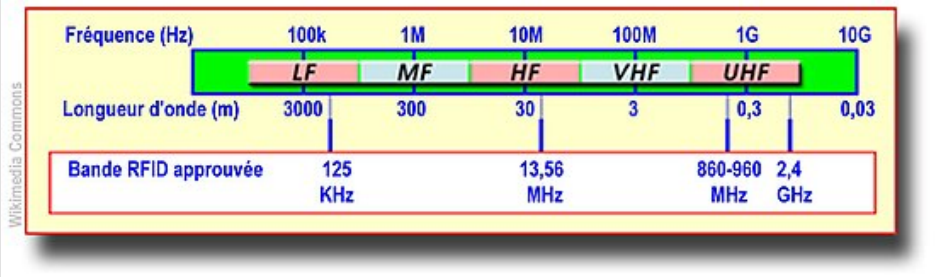
Ces tags sont particulièrement fins, les antennes boucle pouvant être imprimées ou gravées. Ils sont utilisés pour des applications de logistique et de traçabilité, par exemple dans le transport et l'identité[39] : passeport, badge de transport comme le pass Navigo, badge de ski, cartes sans contact, contrôle d'accès des bâtiments, etc. Cette technologie est à la base des applications NFC (Near Field Communication), de plus en plus fréquentes dans les smartphones. La fréquence autorise une lecture à une distance de l'ordre du mètre, mais elle est sensible à la proximité de métaux ou de liquides[40].

- Ultra haute fréquence
  - Ces fréquences ne sont pas harmonisées dans toutes les régions du monde, variant entre 860 et 960 MHz : 915 MHz aux États-Unis, de 865 MHz à 868 MHz dans l'Union européenne pour l'UHF (EPCglobal (en) et ISO 18000-6c). Les fréquences et les puissances d'émission dépendent des

législations. En conséquence, les tags doivent généralement présenter des bandes passantes importantes qui réduisent leurs performances[39].

Une application est par exemple le suivi des trains[41].

- Supra-haute fréquence
  - 2,45 GHz ou 5,8 GHz (micro-ondes) ont des portées de plusieurs mètres, utilisées pour le télépéage notamment.



Bandes autorisées et possibles de fréquences pour les puces RFID communément commercialisées

Gammes de fréquences les plus utilisées et quelques applications RFID [42, 43, 33]

Familles de fréquences	Bandes de fréquences	Régulations	Portée	Taux de transfert[44]	Capacité de lecture près du métal ou des surfaces mouillées[44]	Type de couplage[45]	ISO/CEI 18000	Applications typiques[44, 45]
LF	120–150 kHz	Non régulé	10 cm-50 cm[38]	Lent	Le meilleur	Couplage inductif	ISO/CEI 18000-Partie 2	Suivi des animaux, gestion des accès
HF	13,56 MHz	Bande ISM	10 cm–1 m	Lent à moyen	Moyen (Susceptibilité au métal)[46]	Couplage inductif	ISO/CEI 18000-Partie 3	Suivi des bagages, des livres dans les bibliothèques, surveillance électronique d'articles, porte-monnaie électronique, contrôle d'accès
UHF	433 MHz	Appareils de courte portée	1–100 m	Moyen à rapide	Mauvais	Couplage électrique	ISO/CEI 18000-Partie 7	Suivi dans la chaîne d'approvisionnement et gestion d'entrepôt, applications pour la défense
UHF	865-868 MHz (Europe) 902-928 MHz (Amérique du Nord)	Bande ISM	1–12 m	Rapide	Mauvais	Couplage électrique	ISO/CEI 18000-Partie 6	Code-barres EAN, suivi de chemin de fer[41], système de télécommande
SHF	2450-5 800 MHz	Bande ISM	1–2 m	Très rapide	Le pire	Couplage électrique	ISO/CEI 18000-Partie 4	Télépéage, suivi de chemin de fer, 802.11 WLAN, standards Bluetooth
ULB	3.1–10 GHz	ULB	Supérieur à 200 m	Très rapide	-	Couplage électrique	Non défini	-

Une fréquence élevée favorise un échange d'informations (entre lecteur et marqueur) à des débits plus importants qu'en basse fréquence, et à une distance de lecture plus grande. Avec des débits importants, de nouvelles fonctionnalités au sein des marqueurs (cryptographie, mémoire plus importante, anti-collision) peuvent être ajoutées. Par contre une fréquence plus basse bénéficie d'une meilleure pénétration dans la matière[47].

Le lecteur et le tag sont équipés d'antennes qui doivent s'adapter à l'environnement. De plus, la RFID doit cohabiter d'un point de vue spectral avec d'autres technologies sans fil[48].

L'anti-collision est la possibilité pour un lecteur de dialoguer avec un marqueur lorsque plus d'un marqueur se trouvent dans son champ de détection. Des algorithmes d'anti-collision sont décrits par les normes (ISO 14443, ISO 15693 et ISO 18000).

Principaux types de lecteurs

Les lecteurs sont de différents types[33] :

- les lecteurs mobiles sont habituellement montés sur les chariots élévateurs, et offrent une mobilité et une flexibilité dans les applications de type gestion d'entrepôts ;
- les lecteurs fixes servent majoritairement dans les configurations de type portiques ou convoyeurs ;
- les lecteurs portatifs sont en général utilisés dans la recherche et la localisation de produits dans un entrepôt dont les antennes sont intégrées directement dans le dispositif.

Lecteur portatif RFID universel pour 125 kHz, 134 kHz et 13,56 MHz.

Lecteur portatif RFID Bluetooth pour NeoTAG - KTS, pour 13,56 MHz.

Medea, un lecteur RFID UHF de la société Nordic ID et de puissance 630 mW.

LogiScan, un lecteur Android 5.1.

Portail RFID.

Radio-étiquettes

Le transpondeur RFID détient l'information (par exemple, prix du produit, nom du manufacturier, date de péremption) sur une puce électronique miniaturisée, associée à une antenne qui transmet l'information vers le lecteur RFID via la fréquence radios[34].

Le marqueur se compose :

- d'une antenne ;
- d'une puce de silicium ;
- d'un substrat ou d'une encapsulation.

Un tag RFID est composé d'une antenne conçue pour fonctionner dans une bande de fréquence donnée, connectée à une puce électronique qui stocke les données. Un circuit d'adaptation est nécessaire dans certains cas pour adapter l'impédance de l'antenne à celle de la puce[46].

La capacité d'information standard d'une étiquette RFID est de 2 kB, mais la plupart ne contiennent qu'un numéro d'identification de 96 ou 128 bits[49,50].

Étiquettes RFID utilisées dans les bibliothèques : étiquette carrée pour livres, étiquette ronde pour CD/DVD et étiquette rectangulaire VHS

Outre de l'énergie pour l'étiquette, le lecteur envoie un signal d'interrogation particulier auquel répond l'étiquette. L'une des réponses les plus simples possibles est le renvoi d'une identification numérique, par exemple celle du standard EPC-96 qui utilise 96 bits. Une table ou une base de données peut alors être consultée pour assurer un contrôle d'accès, un comptage ou un suivi donné sur une ligne de montage, ainsi que toute statistique souhaitée.

Le marqueur est extrêmement discret par sa finesse (parfois celle d'une feuille de Rhodoïd), sa taille réduite (quelques millimètres), et sa masse négligeable. Il est fabriqué par des technologies d'électronique imprimée. Son coût étant devenu minime, on peut envisager de le rendre jetable, bien que la réutilisation soit plus écologique.

Les tags RFID sont classés en fonction du mode d'alimentation, de la fréquence d'utilisation, de la capacité cryptographique, du protocole de communication, de la présence ou non d'une puce électronique[46], de la performance de communication, des propriétés en lecture ou écriture, du prix[44].

Modes d'alimentation

Tag passif

Dénués de piles, ces tags tirent leur énergie des ondes magnétiques ou électromagnétiques émises par le lecteur au moment de leur interrogation[30]. Ils rétromodulent l'onde issue de l'interrogateur pour transmettre des informations. Ils n'intègrent pas d'émetteurs RF[51]. La rétention des données est estimée à 10 ans et 100 000 cycles d'écriture[37].

Ils sont peu coûteux à fabriquer : leur coût moyen de 2007 à 2016 se situe entre 0,10 € et 0,20 € [52], [53], [54], [55], et varie de 0,05 €[55] au minimum à 1,5 €[3]. Ils sont généralement réservés à des productions en volume.

La lecture des puces passives va jusqu'à 200 mètres[réf. souhaitée] grâce à la technologie utilisée dans les systèmes de communication avec l'espace bilointain (contre 10 mètres[réf. souhaitée] auparavant[Quand ?]).

Tag semi-actif

Les étiquettes semi-actives (aussi appelées semi-passives ou encore BAP, *Battery-Assisted Passive tags*, en français marqueurs passifs assistés par batterie) utilisent l'énergie du lecteur pour générer la réponse à une requête lecteur. Elles agissent comme des étiquettes passives au niveau communication. En revanche, les autres éléments de la puce tels que le microcontrôleur et la mémoire tirent leur énergie d'une pile[39]. Cette batterie leur permet, par exemple, d'enregistrer des données lors du transport. Les étiquettes sont utilisées dans les envois de produits sous température contôlée et enregistrent la température de la marchandise à intervalles réguliers.

Ces tags sont plus robustes et plus rapides en lecture et en transmission que les tags passifs, mais ils sont aussi plus chers[36].

Tag actif

Les étiquettes actives sont équipées d'une batterie pour émettre un signal. De ce fait, elles peuvent être lues à longue distance (100 m environ)[44], contrairement aux marqueurs passifs. En général, les transpondeurs actifs ont une grande capacité de mémoire pour stocker des informations telles que le connaissement (128 Kb et plus)[56]. Ils sont principalement utilisés dans des applications de télémétrie, pour communiquer un grand nombre d'informations sur de grandes distances[3].

Cependant, une émission active d'informations signale à tous la présence des marqueurs et pose la question de la sécurité des marchandises. Autre limitation, leur durée de vie est de 5 ans au maximum. Ces tags sont généralement plus chers (15 à 40 € en 2007)[57]. Le risque de collision de la fréquence d'opération du transpondeur avec des ondes électromagnétiques usuelles est élevé, ce qui limite également la localisation très fine des produits[56].

Les étiquettes sans puce font leur apparition. Comme leur nom l'indique, elles ne disposent pas de circuit électronique. C'est l'impression de l'étiquette, basée sur des principes physiques ou chimiques qui engendre un identifiant unique[3]. D'un coût très faible, ces dernières constituent une alternative aux code-barres[58]. Un exemple d'étiquette sans puce est le tag SAW (*surface acoustic wave*, onde acoustique de surface)[59].

Contraintes

Éthique, vie privée et règlementation

Dans le Monde

Dans les années 2000, les puces RFID se banalisent dans les pays industrialisés. En 2010, l'implantation de micropuces « chez l'homme se pratique (exemple : puce VeriChip ou « *code barre humain* »), avec le risque corrélatif de formes de contrôle de l'individu et de la société »[60]. Et ce avant même que la législation n'ait eu le temps de s'appuyer sur une réflexion éthique approfondie, notamment concernant les dispositifs actifs ou passifs et de plus en plus miniaturisés (en 2006 déjà, Hitachi propose une puce carrée de 0,15 × 0,15 mm ; plus petite que le diamètre de certains cheveux[61]). Implantables ou implantés dans le corps humain[60] (une société allemande, Ident Technology[62], met au point des dispositifs faisant de la peau humaine, animale vivante ou d'autres parties du corps un transmetteur de données numériques)[60], dans ou sur les vêtements (*wearable computing* ou *cyber-vêtement*) et dans les objets communicants ; ces puces sont autant d'innovations qui sont sources de questions éthiques et de risques de dérives[63,64].

Si leur utilité ne fait pas de doute dans de nombreux domaines, les dangers de l'implantation de la puce inquiètent. En 2006, le ministère de l'intérieur américain déconseille les puces RFID pour l'identification humaine[65] [réf. à confirmer].

Le principal risque est l'atteinte à la vie privée de l'utilisateur. En effet, si l'identifiant de la puce est relié à l'identité de la personne implantée, alors il est possible de suivre toutes ses actions chaque fois que la puce est activée dans le champ d'un lecteur. De plus, cette puce étant une invention récente, depuis 2004[66], elle est comparée à l'internet des débuts, c'est-à-dire à un internet non sécurisé. La RFID peut donc être facilement « hackée » malgré son cryptage. Les experts [Qui ?] révèlent qu'il existe des failles dans la confection de la puce et que celle-ci peut être détournée de son utilisation première [réf. nécessaire].

Des chercheurs s'interrogent sur l'évolution de l'usage de la puce[67].

En Europe

Après un rapport de 2005 sur les nouveaux implants dans le corps humain[68] et après une table ronde organisée par le GEE (Groupe européen d'éthique des sciences et des nouvelles technologies)[69] fin 2004 à Amsterdam[70], la Commission européenne demande un avis au Groupe interservice sur l'éthique, dont le secrétariat[71] est assuré par le BEPA (Bureau des conseillers de politique européenne)[72]. Il travaille en lien avec le Groupe européen d'éthique des sciences et des nouvelles technologies[73] qui, à la demande du GEE, émet le 16 mars 2005 un avis intitulé « Aspects éthiques des implants TIC dans le corps humain »[60].

Les droits fondamentaux concernés sont la Dignité humaine, le Droit à l'intégrité de la personne, la Protection des données à caractère personnel (voir la Charte des droits fondamentaux de l'Union européenne[74]).

La question touche aussi la santé publique, la protection de la vie privée dans les communications électroniques[75], la législation sur les dispositifs médicaux implantables actifs[76], le consentement et le droit à l'information[77], la protection du génome humain[78], la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[79], les possibles utilisations abusives[80].

En mai 2009, la Commission européenne publie une recommandation[81] axée sur la désactivation systématique des tags RFID au point de vente. Pour les applications ne désactivant pas systématiquement les tags, la mise en service de l'application RFID est soumise à la réalisation d'une évaluation d'impact sur la vie privée (EIVP ou Privay Impact Assessment, PIA en anglais). En juillet 2014, une norme européenne est publiée (EN 16571) qui donne la méthodologie à suivre pour réaliser une EIVP. Le rapport d'EIVP doit être transmis à l'organisme chargé de la protection des données à caractère personnel (en France, la CNIL) 6 semaines avant la mise en service de l'application.

En France

Puisque ces puces RFID collectent des données personnelles, la Commission nationale informatique et libertés (CNIL) pose un regard sur ces pratiques en droit français.

En France où existe conformément à la législation européenne un droit à l'intégrité physique, la CNIL s'inquiète dans son rapport annuel du 16 mai 2008[82] des risques de traçabilité des individus qui n'ont pas accès à leurs données.

Si la CNIL ne possède qu'un pouvoir de recommandations, des textes juridiques non contraignants, elle peut infliger des sanctions. Ces sanctions se présentent sous la forme d'amendes aux entreprises qui ne respecteraient pas les principes de base de la protection des données personnelles.

En droit français, il existe toutefois la loi contraignante du 6 janvier 1978 dite « loi Informatique et Libertés »[83]. Cette loi peut s'appliquer puisque les puces RFID identifient directement ou indirectement une personne physique. L'application de la loi à ce type de radio-identification est confirmée en juillet 2010 par le G29. Le G29 est un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales dans 28 pays en Europe et dont la France fait partie.

La recommandation du 12 mai 2009 de la Commission européenne préconise que les exploitants de dispositifs de radio-identification évaluent l'impact sur la vie privée ; l'étude se présente sous forme de liste des risques identifiés en matière de vie privée et les mesures prises pour traiter ces risques ; elle est applicable en France[84].

De plus, depuis septembre 2006, un arrêté de l'Autorité de régulation des communications électroniques et des postes qui avait fixé les modalités d'utilisation des étiquettes autorise la libre utilisation de la bande de fréquence 865-868 MHz pour les dispositifs RFID.

Si ces principes demeurent généraux et peu contraignants notamment dans le cas de dispositifs de radio-identification des salariés des entreprises, les règles du Code du travail sont applicables.

En effet, l'article L.1121-1 du Code du travail dispose que « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Les puces RFID implantées sous la peau des salariés entrent dans ce cadre puisque utilisées pour accéder à des locaux, effectuer les tâches de bureau ou acheter des boissons ou nourritures dans les distributeurs ; la radio-identification peut facilement être remplacée par un dispositif moins invasif pour la vie privée. Ainsi, ces puces RFID ne sont ni justifiées par le peu d'importance des tâches à accomplir, ni proportionnées au but recherché, à savoir une facilitation de déplacement et d'utilisation des services d'une entreprise[85].

La Cour de cassation, haute juridiction française, se prononce sur cette question le 17 décembre 2014. Les juges considèrent que le recours à la géolocalisation des salariés n'est pas justifié lorsque les salariés ne disposent pas de liberté dans l'organisation de leur travail et lorsque le contrôle pourrait être fait par un autre moyen[86]. Par exemple, si le salarié doit justifier de sa présence dans l'entreprise par la détection par un logiciel de sa puce lorsqu'il est présent dans les locaux alors qu'il pourrait simplement utiliser un badge classique et passer ce dernier sur une "badgeuse", système ancien contrôlant les entrées et sorties des salariés ainsi que leur temps de travail.

Par ailleurs, Jacques Attali, dans l'émission « Conversation d'avenir », la RFID (Public Sénat)[87], suggère que ces puces soient implantées, volontairement ou sans le savoir, sur des immigrants, des prostituées qui tentent d'échapper à leurs souteneurs, afin que celles-ci soient localisées dans un but de protection.

Obstacles

Environnement métallique

La lecture de radio-étiquettes posées sur des objets à l'intérieur d'un conteneur métallique est plus difficile. Un plan de masse modifie l'accord de l'antenne du tag. ; la distance de lecture est réduite considérablement. De nouvelles familles de tags intègrent un plan métallique dans le design de l'antenne, ce qui maintient des distances de lecture proches de celles observées sur des supports neutres. Dans tous les cas, un tag à l'intérieur d'une enceinte métallique ne peut pas être lu par un lecteur situé à l'extérieur. C'est l'effet de cage de Faraday, qui réalise un blindage électromagnétique.

Collisions

Lorsque plusieurs marqueurs se trouvent dans le champ d'un lecteur, les communications sont brouillées par l'activité simultanée des marqueurs.

La détection de la collision est en fait une détection d'erreur de transmission, à l'aide d'un bit de parité, d'une somme de contrôle ou d'une fonction de hachage. Dès qu'une erreur est détectée, l'algorithme d'anticollision est appliqué.

Plusieurs méthodes d'anticollision sont développées. Voici les quatre principales :

- la méthode fréquentielle : chaque marqueur communique sur une plage de fréquences spécifique avec le lecteur. En pratique, c'est inutilisable à grande échelle ;
- la méthode spatiale : avec une antenne directionnelle et à puissance variable, le lecteur couvre petit à petit chaque partie de l'espace pour communiquer avec chaque marqueur et l'inhiber avant de le réactiver pour ensuite communiquer avec lui. En pratique, la présence de deux marqueurs à faible distance l'un de l'autre rend cette méthode inefficace ;
- la méthode temporelle : le lecteur propose aux marqueurs une série de canaux de temps dans lesquels ils répondent. Les marqueurs choisissent de façon aléatoire leur canal de temps. Si un marqueur est seul à répondre dans un canal, il est détecté et inhibé par le lecteur. Si plusieurs marqueurs répondent en même temps, il est nécessaire de répéter l'opération. Peu à peu, tous les marqueurs sont connus et inhibés ; il suffit alors au lecteur de réactiver le marqueur avec lequel il souhaite communiquer. En pratique, le côté aléatoire rend inconnue la durée de la méthode ;
- la méthode systématique : de nombreux brevets décrivent des méthodes systématiques. Tous les marqueurs sont détectés et inhibés en parcourant l'arbre de toutes les possibilités d'identifiants (par exemple, le lecteur envoie une requête du type « Tous les marqueurs dont le premier bit d'identification est 1 doivent se manifester. » Si un seul marqueur se manifeste, le lecteur l'inhibe, et s'intéresse ensuite aux marqueurs avec pour premier bit 0, et ainsi de suite). En pratique, cette méthode s'avère longue.

Utilisations

Marquage d'objets

Clef électronique RFID de réception Keymate.

- Système implanté d'identification et mémorisation : de manière courante, des puces basse fréquence (125 à 135 kHz) sont utilisées pour la traçabilité d'objets (ex : fûts de bière). La traçabilité des livres dans les librairies et les bibliothèques, la localisation des bagages dans les aéroports utilisent plutôt la classe haute fréquence (13,56 MHz).
- Suivis industriels en chaîne de montage.
- Peu connue mais en expansion, la RFID dans la gestion rationnelle des déchets ménagers a pour but une tarification incitative[88] .
- Contrôle d'accès : il se fait par badge de *« proximité »* ou *« mains-libres »*.
  Certaines *« clés électroniques »* d'accès sont des marqueurs pour la protection « *sans serrures* » de bâtiments ou de portières automobiles. Les badges mains-libres sont utilisés jusqu'à 150 cm selon le type d'antenne. Ils contiennent une Identité numérique ou un certificat électronique ; ils donnent l'accès à un objet communicant ou à son activation.
  Dans l'accès à des bâtiments sensibles la radio-identification remplace les badges magnétiques ; les personnes sont authentifiées sans contact. La radio-fréquence de la plupart des badges d'accès n'a une portée que de quelques centimètres, mais ceux-ci ont l'avantage de la lecture-écriture dans la puce, pour mémoriser des informations (biométriques, par exemple).

Clé électronique pour système de serrure RFID.

- Traçabilité distante d'objets fixes ou mobiles, comme des palettes et conteneurs dans des entrepôts ou sur les docks suivis via des marqueurs UHF (ultra haute fréquence).
- Inventaires : Une analyse[89] effectuée chez Wal-Mart a démontré que la radio-identification peut réduire les ruptures d'inventaire de 30 % pour les produits ayant un taux de rotation entre 0,1 et 15 unités/jour. Saisie automatique d'une liste de produits achetés ou sortis du stock.
  À cette fréquence, la lecture n'est théoriquement pas possible à travers l'eau (ni donc à travers le corps humain). Cependant lors des *RFID Journal Awards 2008*, l'entreprise Omni-ID présente une étiquette RFID lisible à travers l'eau et à proximité de métal, avec un taux de fiabilité de 99,9 %.

- Antivols utilisés dans les magasins, notamment pour la lutte contre la contrefaçon. Des étiquettes RFID antivol sont présentes directement sur les emballages ou sur les produits dans les étalages.
- Traçabilité d'aliments : dans la chaîne du froid, une puce peut théoriquement enregistrer les variations de température des aliments. Il existe un réfrigérateur capable de reconnaître automatiquement les produits qu'il contient, mais aussi capable de contrôler les dates limites d'utilisation optimale (DLUO) des produits alimentaires périssables.
- Identification de containers de substances chimiques, de médicaments[90].
- Identification de mobilier urbain, jeux publics, d'arbres d'ornement pour maintenance et suivi[91].
- Échange de cartes de visites lors d'évènements[92].
- Télépéages d'autoroutes.
- Des marqueurs micro-ondes (2,45 GHz) contrôlent l'accès à longue distance de véhicules, comme sur de grandes zones industrielles. Ces marqueurs sont généralement actifs.
- Contrôle des forfaits de remontée mécanique dans les stations de sport d'hiver.
- Rechargement de véhicules électriques[93].

Transactions financières

Les systèmes de **paiement sans contact** tels que des cartes de crédit, des porte-clés, des cartes à puce ou d'autres dispositifs (téléphone mobile…) utilisent la technologie radio frequency identification et Near Field Communication pour des paiements sécurisés. Avec une puce intégrée et une antenne les consommateurs paient avec leur carte (sans contact) sur un lecteur au point de vente.

Carte et terminal de paiement sans contact.

Certains fournisseurs affirment que les transactions sont presque deux fois plus rapides qu'une transaction classique[94]. Il n'y a ni signature, ni saisie du code PIN pour les achats de moins de 25 $ US aux États-Unis, moins de CHF 40 en Suisse et moins de 50 € pour la France.

À Hong Kong et aux Pays-Bas des marqueurs sous forme de carte de crédit sont répandus comme moyen de paiement électronique (équivalent de Moneo en France). Ils sont utilisés à Bruxelles comme titre de transport sur le réseau de STIB (voir MoBIB) et désormais en France, à travers le paiement sans contact de Cityzi, expérimentés à Nice depuis 2010[95].

Marquage d'êtres vivants

- Identification de plantes (arbres de la ville de Paris), d'animaux d'élevage (vaches, cochons) ou de compagnie comme les chats et les chiens (grâce à une puce implantée sous la peau dans le cou), d'animaux sauvages (cigognes, manchots) : ce sont généralement des puces basse fréquence (125 à 135 kHz). Suivi d'un cheptel : nourriture, lactation, poids[96] [source insuffisante] ; l'identification des animaux[97] grâce à l'implantation d'une puce (déjà obligatoire en Belgique et en Suisse pour les chiens et les chats) ; obligatoire en France pour tous les équidés depuis le 1er janvier 2008 ;l'identification des adresses postales (UAID), des cartes d'identité (INES) ;
- La lutte contre la contrefaçon avec des puces plus difficiles à imiter que les code-barres.
- Relevés scientifiques : des marqueurs collectent des données issues des relevés (monitoring) produits dans un organisme ou par des stations de mesure isolées et autonomes (stations météorologiques, volcaniques ou polaires). Des laboratoires de recherche et des bureaux d'étude utilisent cette technologie pour suivre les déplacements des poissons dans des rivières contraintes par des obstacles physiques (seuil, barrages, buses souterraines ...). En équipant les poissons, on identifie les obstacles limitant leur déplacement[98]; on évalue l'efficacité des ouvrages de correction pour leur liberté de circulation, comme des passes à poisson ou des buses aménagées[99].
- Chez l'Homme : des radio-marqueurs sous-cutanés, originellement conçus pour la traçabilité des animaux, peuvent sans aucune contrainte technique être utilisés sur des humains. Ainsi, l'artiste américain Eduardo Kac est le premier humain à recevoir un implant de puce électronique sous-cutanée RFID en 1997[100, 101]. Kac s'est implanté une micropuce en direct à la télévision et sur Internet dans sa performance *Time Capsule*[102]. La société *Applied Digital Solutions* propose ses radio-marqueurs sous-cutanés (nom commercial : VeriChip) destinés à des humains, pour identifier les fraudes, assurer l'accès protégé à des sites confidentiels, le stockage des données médicales et aussi pour résoudre rapidement des enlèvements de personnalités. Combinés à des capteurs sensibles aux fonctions principales du corps humain, ces systèmes sont un moyen de supervision de l'état de santé d'un patient.

Une boîte de nuit de Barcelone (Baja Beach Club) offre à ses clients VIP une fonction de porte-monnaie électronique implanté dans leur corps même avec des puces sous-cutanées.
La ville de Mexico implante cent soixante-dix radio-marqueurs sous la peau de ses officiers de police pour contrôler l'accès aux bases de données et aussi pour les localiser en cas d'enlèvement[103].

Marché des RFID

En 2010, le marché mondial des étiquettes RFID s'élève à environ 5,6 milliards de dollars américains[109]. Ce marché a quasiment doublé en 5 ans pour atteindre 9,95 milliards de dollars en 2015[108] et continue de croître à 10,52 milliards de dollars en 2016 et est estimé à 11,2 milliards de dollars en 2017[108]. Ces chiffres incluent tous les types de RFID, actif et passif, sous toutes les formes : étiquettes, cartes, lecteurs, logiciels et services pour les étiquettes RFID, etc. IDTechEx fait une estimation à 14 milliards de dollars en 2020[110] et à 14,9 milliards de dollars en 2022[108], notamment grâce à l'adoption accrue du RFID dans les vêtements, qui occupe déjà en 2015 environ 80 % du volume du marché pour les étiquettes RFID passives[110].

Pour des raisons techniques, il est temporairement impossible d'afficher le graphique qui aurait dû être présenté ici.

Marché total du RFID entre 2009 et 2017 [104], [105], [106], [107], [108].

Cette croissance continue du marché s'effectue cependant à un rythme plus lent que celui estimé : le site d'étude de marché et statistiques Statista prévoyait en 2010 que le marché atteindrait 11,1 milliards de dollars dès 2015[109], ce seuil n'est atteint que 2 ans plus tard, en 2017[108]. IDTechEx supposait, en 2006, que le marché total du RFID s'élèverait à 26,23 milliards de dollars en 2016[111], soit plus du double qu'atteint effectivement cette année là[108].

En 2005, IBM dénombre 4 millions de transactions RFID chaque jour. En 2010, ce constructeur évalue à environ 30 milliards le nombre d'étiquettes RFID produites dans le monde et 1 milliard de transistors par être humain[112]. Au total, 34 milliards d'étiquettes RFID (33 milliards de passif) sont vendues depuis que la RFID a commencé à avoir des premiers usages en 1943[110]. 7,5 milliards d'étiquettes ont été consommées durant l'année 2014 seule[108]. Malgré cela, environ 99 % du marché disponible est inexploité en 2012[109]. En 2019, le marché d'étiquettes est passé à 20,1 milliards[113].

Applications

Applications existantes

Puce RFID intégrée dans la poubelle.

- Accès aux transports publics : Nantes (carte Libertan), Marseille (carte transpass), Lille et région Nord-Pas-de-Calais (Pass Pass), Paris (Carte Navigo), Toulouse (Carte Pastel), Rennes (carte KorriGo), Reims (Carte Grand R et tickets unitaires), Nancy, TER Lorraine, Troyes (Busséo), Bruxelles (pass MoBIB), Montréal, Luxembourg, Strasbourg (Carte Badgéo), Le Mans (Carte Moovéa), Lyon (Carte Técély), région Rhône-Alpes (Carte OùRA!), Venise (carte imob.venezia), TER Rhône-Alpes, Nimes (carte BANG) Suisse (Swisspass CFF).
- Guidage des personnes. L'office de tourisme des Hautes Terres de Provence (Alpes-de-Haute-Provence) a créé des promenades où les familles vont de lieux en lieux, en glanant des indices que leur dévoilent de faux rochers, dans lesquels sont dissimulés des haut-parleurs, qui se mettent en marche lorsqu'une puce (collée sur un livret « magique ») en est approchée.
- Circulation des personnes. À l'université de Cornell, accès des étudiants à la bibliothèque à toute heure sans formalité. En France, la clinique de Montfermeil utilise des bracelets équipés de puce RFID pour prévenir l'enlèvement des nouveau-nés.


FasTrak, une étiquette RFID utilisée pour le télépéage en Californie.


Étiquette RFID cousue dans un vêtement fabriqué par Decathlon. Numérisation avant, arrière et en transparence.

- Bibliothéconomie. Bibliothèque de Rennes Métropole au Champs Libres, bibliothèque de Cornell, bibliothèques des Pays-Bas (puce SLI de Philips). Identification de livres pour enfants par le Nabaztag:tag pour téléchargement des livres audio correspondants.
- Parcs de véhicules. Vélos de Vélib' à Paris et de Vélo'v à Lyon, autopartage[114].
- Épreuves sportives. Marathon de Paris, semi-marathon Marseille-Cassis), Tour de France). Les puces sont fixées sur une chaussure, un cadre de vélo, ou le dossard des participants pour le chronométrage individuel lors du passage des lignes de départ et d'arrivée.

Puce de radio-identification à fixer sur une chaussure.

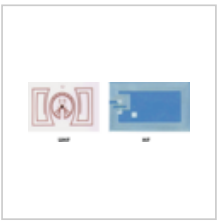
Évolution

Les étiquettes « intelligentes » sont souvent envisagées comme un moyen de remplacer et d'améliorer les codes-barres de la norme UPC/EAN. Les radio-identifiants sont en effet assez longs et dénombrables pour donner à chaque objet un numéro unique, alors que les codes UPC utilisés actuellement ne donnent qu'un numéro pour une classe de produits. Les codes-barres UPC/EAN tracent le déplacement des objets depuis la chaîne de production jusqu'au consommateur final. En cela, ils sont considérés par les industriels de la chaîne logistique comme la solution technologique ultime à tous les problèmes de traçabilité, notion essentielle depuis les crises sanitaires liées aux filières alimentaires.

Cependant, les solutions de radio-identification souffrent d'un manque de normalisation. La jungle des solutions rend la traçabilité universelle difficile à réaliser.

EPCglobal[115] est une organisation qui travaille dans ce sens sur une proposition de standard international pour les usages techniques de radio-identification. Le but est d'avoir un système de distribution homogène des identifiants afin de disposer d'un EPC (*electronic product code* ou code produit électronique) pour chaque objet présent dans la chaîne logistique de chaque entreprise du monde.

Galerie

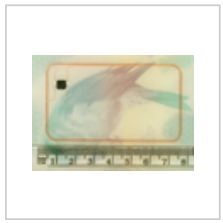


Antennes d'étiquettes UHF et HF.

Matériel d'insertion et puce d'identification animale (fréquence : 2 kHz).

Lecteur et puce insérée dans le cou d'un chien.

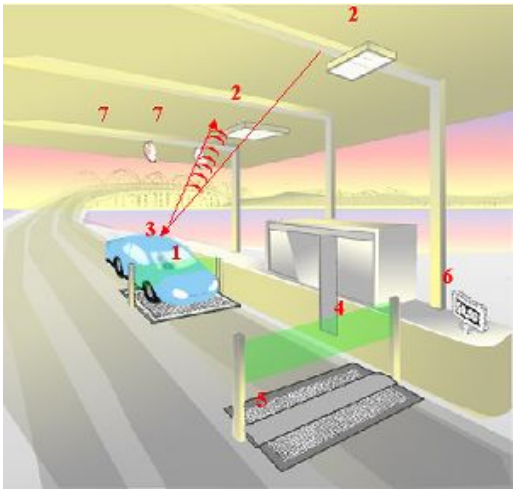
Puce RFID encapsulée, de 5 cm (125 kHz).



BMicro-puce contenant des données biométriques, insérée dans un passeport.

Puce RFID passive (Chip Rfid Ario 370DL) en « bouton », adaptée aux uniformes et textiles (résistance aux traitements en blanchisseries).

Transpondeur *Fast-track* sur un pare-brise, utilisé par exemple pour le péage urbain (accroche velcro).



Péage *FasTrak* **(en)** californien (de « *fast trak* », « voie rapide » en français), un système de télépéage automatique, sans arrêt du véhicule.

Dans la voie de péage, des capteurs (1) détectent le véhicule, lisent (2) le transpondeur (3) monté sur le pare-brise. Le « rideau de lumière » (4) compte (5) le nombre d'essieux, et le compte-propriétaire de la puce est facturé. Un panneau électronique (6) affiche le prix facturé. Un véhicule sans transpondeur est classé comme contrevenant ; les caméras (7) filment et mémorisent la plaque d'immatriculation pour une contravention (si la plaque est celle d'un utilisateur FasTrak enregistré, il ne paiera que le prix du péage).

Empreinte environnementale

À l'instar de toute production industrielle, la production de puces RFID consomme des ressources naturelles et produit des gaz à effet de serre. Il n'y a malheureusement à ce jour que très peu d'études portant sur l'impact environnemental direct de la production et du recyclage de cette technologie[116].

Cependant, la RFID connaît un essor, notamment pour répondre aux enjeux environnementaux, au sein des chaînes de production, dans la gestion des déchets ainsi que dans le domaine du transport et de la géolocalisation.

Ainsi, par exemple, dans certaines villes européennes, les poubelles résidentielles sont équipées de puces RFID. Les camions poubelles, équipés de lecteurs RFID, identifient les poubelles ramassées grâce à leur puce[117]. Cette gestion des déchets par RFID permet une surveillance de leur nature et de leur quantité pour une optimisation de leur traitement.

Dangers

Les technologies de radio-identification pourraient s'avérer dangereuses pour l'individu et la société (ex. : santé et protection de la vie privée)[118], avec :

- atteinte à la vie privée dans le cas de marqueurs « furtifs » ou accessibles à des systèmes susceptibles de diffuser des informations sur la vie privée ;
- utilisation d'informations contenues par les marqueurs de passeports pour agresser sélectivement et par simple proximité physique les ressortissants de certaines nationalités ;
- « marquage » de personnes ayant acheté ou emprunté certains types de films, livres (politique, religion, etc.) comme « indésirables » dans les fichiers d'employeurs ou d'un État répressif (possible à l'heure actuelle sans cette technologie) ;
- « souveraineté numérique/économique » liée à l'infrastructure du réseau EPCGlobal, notamment s'agissant de l'administration, par contrat, de sa racine (onsepc.com) par un acteur privé (américain) ;
- éthique et droit à l'intégrité physique de la puce sous-cutanée. La limitation au volontariat et au consentement éclairé ne garantit pas le respect de la vie privée (cf. charte des droits de l'homme, et en Europe, Charte des droits fondamentaux de l'Union européenne) ; dans certains contextes des personnes refusant ces étiquettes sous-cutanées risquent d'être victimes de discriminations ;
- identification de personnes par une signature de l'ensemble des étiquettes d'identification par radiofréquences (cartes bancaires, téléphone mobile, pass de transports en commun…) habituellement portées (cf. brevet IBM : Identification and Tracking of Persons Using RFID Tagged Objects par ex.) ;
- au-delà d'un certain seuil de concentration, l'émission de signaux radio-fréquences s'avérerait dangereuse pour la santé (effets suspectés d'un smog électromagnétique croissant…), après la constatation d'interférences perturbant le fonctionnement des appareils bio-médicaux[119].

Dans un rapport publié le 26 janvier 2009[120], l'AFSSET recommande de poursuivre la veille scientifique sur la recherche d'effets biologiques des rayonnements liés au RFID.

Protection de l'individu

La législation française prévoit une certaine protection de la vie privée en interdisant :

- le contrôle clandestin (toute identification doit faire l'objet d'une indication visible) ;
- l'usage des mêmes appareils pour le contrôle d'accès et le contrôle de présence.

Selon l'association allemande FoeBuD, la législation n'est pas assez restrictive pour la technologie de radio-identification et la protection des informations personnelles[121].

Certaines associations proposent des outils pour se protéger d'une utilisation non autorisée de la radio-identification, tels que RFID Guardian[122].

D'autres associations proposent le boycott de cette technologie qu'elles estiment liberticide[123]. Selon elles, le fichage d'informations non contrôlables dans une carte d'identité électronique serait préjudiciable à la liberté des individus[124].

Logo de la campagne anti-RFID du groupe allemand digitalcourage (anciennement FoeBuD).

En 2006, un groupe de hackers déclare à la convention bi-annuelle Sixth HOPE à New York avoir cracké (cassé) les sécurités de la fameuse puce sous-cutanée[125]. Les hackers prétendent aussi avoir pu la cloner[126]. Ils estiment que la législation est trop souple avec cette technologie, au regard de son potentiel d'atteinte à la vie privée et de fuite d'information.

Certains sacs à main possèdent une poche anti-RFID, pour les cartes de crédit et les passeports, qui empêche l'accès non autorisé aux informations personnelles.

Certains outils protègent les données sensibles présentes sur les cartes RFID. Il est aujourd'hui très simple de copier ou récupérer des données présentes sur des badges ou cartes RFID grâce à un capteur de tag RFID. Un étui anti-piratage pour carte RFID protège les données grâce à sa composition en métal bloquant les ondes magnétiques et donc le piratage.

Protection des données personnelles

Ces dispositifs de radio-identification collectent, ou plus simplement contiennent, des informations personnelles sur la personne sur laquelle la puce est implantée. Dans le domaine du travail se pose la question de la protection de ces données collectées au sein de l'entreprise. Le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données rend obligatoire la nomination d'un délégué à la protection des données ou « DPO » (initiales de l'anglais « *Data Protection Officer* ») auprès des :

- autorités et organismes publics ;
- structures dans lesquelles les activités de base exigent « un suivi régulier et systématique à grande échelle des personnes concernées » ;
- structures dont le traitement consiste en un « traitement à grande échelle » de données sensibles.

Avant les délégués à la protection des données il existait la fonction de correspondant informatique et liberté (CIL) ; toutefois cette fonction n'a été que très peu utilisée en pratique. Le caractère d'obligation concerne plus d'entreprises. De plus dès lors que des données sont traitées, il est recommandé aux entreprises de nommer un DPO même si ce n'est pas obligatoire.

L'une des principales nouveautés liée à cette fonction est qu'il faut avoir des « connaissances spécialisées du droit » et des « pratiques en matière de protection des données ».

Le délégué a un rôle crucial. En effet, dans une entreprise une implantation de puces contrôlerait la durée du travail des salariés, leur donnerait accès au restaurant d'entreprise mais fournirait des informations de base sur leur identité. Certaines informations relevant de la sphère privée il est dès lors indispensable qu'une protection soit mise en place, d'autant plus au niveau européen.

Une sécurité certifiée

L'ANSSI délivre le 24 octobre 2013 pour la première fois la Certification de sécurité de premier niveau (CSPN) pour le lecteur RFID LXS W33-E/PH5-7AD, version 1.1 développé par la société Systèmes et Technologies Identification (STid)[127]. Cette certification garantit à l'acquéreur un produit répondant aux exigences de sécurité de la Certification de sécurité de premier niveau.

Notes et références

1. legifrance.gouv.fr - décision de la Commission générale de terminologie et de néologie sur le terme français *radio-identification*, le 9 septembre 2006 **[PDF]** (http://www.legifrance.gouv.fr/imagesJOE/2006/0909/joe_20060909_0209_0097.pdf).
2. lefigaro.fr « Le premier homme contaminé par un virus informatique » (http://www.lefigaro.fr/sciences-technologies/2010/05/26/01030-20100526ARTFIG00686-le-premier-homme-contamine-par-un-virus-informatique.php), lefigaro.fr, mai 2010.
3. Anthoy Ghiotto, *Conception d'antennes de tags RFID UHF, application à la réalisation par jet de matière* (Thèse d'exercice), Institut polytechnique de Grenoble, 26 novembre 2008 (lire en ligne (https://tel.archives-ouvertes.fr/tel-00389807/document) **[PDF]**)
4. **(en)** ISECOM, *Hacking Exposed Linux : Linux Security Secrets & Solutions*, McGraw-Hill Osborne Media, 2008, 3e éd., 813 p. (ISBN 978-0-07-226257-5, lire en ligne (https://books.google.com/books?id=f5Vz08spzw8C&printsec=frontcover)), p. 298
5. **(en)** H. Stockman, « Communication by means of reflected power », *Proc. IRE*, vol. 36, n°10, 1948, p. 1196-1204
6. **(en)** F.L. Vernon, « Applications of the microwave homodyne », *Antennas Propag. Trans. IRE Prf. Group On*, vol. 4, n°1, 1952, p. 110-116
7. **(en)** Hunt et D. V., *RFID - A guide to radio frequency identification*, John Wiley & Sons, 2007

8. **(en)** Rajit Gadh, George Roussos, Katina Michael, George Q. Huang, B. Shiv Prabhu et Peter Chu, « RFID - A Unique Radio Innovation for the 21st Century », *Proceedings of the IEEE*, vol. 98, nº 9, septembre 2010, p. 1546-1549 (lire en ligne (https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5552248))
9. Brevet US 2927321 (http://v3.espacenet.com/textdoc?locale=fr_V3&DB=EPODOC&F=0&IDX=US2927321) enregistré le 16 aout 1952, publié le 1er mars 1960
10. **(en)** Donald B. Harris, *Radio transmission systems with modulatable passive responder*, Google Patents, 1960 (lire en ligne (https://patentimages.storage.googleapis.com/95/01/9d/766a2cdbbe1c30/US2927321.pdf))
11. Brevet US 3391404 (http://v3.espacenet.com/textdoc?locale=fr_V3&DB=EPODOC&F=0&IDX=US3391404) enregistré le 18 mai 1959, publié le 2 juillet 1968
12. **(en)** Joseph H Vogelman, *Passive data transmission technique utilizing radar echoes*, Google Patents, 1968 (lire en ligne (https://patentimages.storage.googleapis.com/92/8b/e2/a914cbb0848bce/US3391404.pdf))
13. Brevet US 3299424 (http://v3.espacenet.com/textdoc?locale=fr_V3&DB=EPODOC&F=0&IDX=US3299424) enregistré le 07 mai 1965, publié le 17 janvier 1967
14. **(en)** Jorgen P Vinding, *Interrogator-responder identification system Google Patents*, Google Patents, 1967 (lire en ligne (https://patentimages.storage.googleapis.com/b7/ab/a6/5bab81426be3ac/US3299424.pdf))
15. Brevet US 3460139 (http://v3.espacenet.com/textdoc?locale=fr_V3&DB=EPODOC&F=0&IDX=US3460139) enregistré le 06 septembre 1967, publié le 5 août 1969
16. **(en)** Otto E Rittenbach, *Communication by radar beams*, Google Patents, 1969 (lire en ligne (https://patentimages.storage.googleapis.com/1f/47/ab/b6f14ddf3440ed/US3460139.pdf))
17. **(en)** R. Harrington, « Electromagnetic scattering by antennas », *Antennas Propag. IEEE Trans. On*, vol. 11, nº 5, 1963, p. 595-596
18. **(en)** J. K. Schindler, R. B. Mack et P. Blacksmith Jr, « The control of electromagnetic scattering by impedance loading », *Proc. IEEE*, vol. 53, nº 8, 1965, p. 993-1004
19. Brevet US 3713148 (http://v3.espacenet.com/textdoc?locale=fr_V3&DB=EPODOC&F=0&IDX=US3713148) enregistré le 21 mai 1970, publié le 23 janvier 1973
20. **(en)** Mario W. Cardullo et William L. Parks, *Transponder apparatus and system*, Google Patents, 1973 (lire en ligne (https://patentimages.storage.googleapis.com/4a/63/c4/1e14dedfdb7bd2/US3713148.pdf))
21. **(en)** « Genesis of the Versatile RFID Tag (https://www.rfidjournal.com/article/view/392/1/2) », RFID Journal (consulté le 22 septembre 2013).
22. **(en)** Daniel Dobkin, *RF in RFID : Passive RFID UHF in Practice*, Amsterdam, Newnes, 2008, 2e éd., 529 p. (ISBN 978-0-12-394583-9)
23. **(en)** Himanshu Bhatt et Bill Glover, *RFID Essentials*, O'Reilly, 2006, 260 p. (ISBN 978-0-596-00944-1, lire en ligne (https://books.google.com/books?id=cKKZoH48D4cC&printsec=frontcover))
24. **(en)** Jerry Landt, « Shrouds of Time: The history of RFID (http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf) » **[PDF]**, sur *AIM, Inc.*, 2001 (consulté le 31 mai 2006).
25. **(en)** « Real Time Location Systems (http://www.clarinox.com/docs/whitepapers/RealTime_main.pdf) », clarinox, novembre 2009 (consulté le 4 août 2010).
26. Brevet US 4384288 (http://v3.espacenet.com/textdoc?locale=fr_V3&DB=EPODOC&F=0&IDX=US4384288) enregistré le 31 décembre 1980, publié le 17 mai 1983
27. **(en)** Charles A. Walton, *Portable radio frequency emitting identifier*, Google Patents, 1983 (lire en ligne (https://patentimages.storage.googleapis.com/46/83/72/641c3c743d0c02/US4384288.pdf))
28. Auto-ID Center, « Annonce de la fermeture du Auto-ID Center » (https://web.archive.org/web/20040414231517/http://www.autoidcenter.org/) (version du 14 avril 2004 sur *Internet Archive*)
29. « Introduction à la RFID » (https://web.archive.org/web/20171213025942/http://www.centrenational-rfid.com/introduction-a-la-rfid-article-15-fr-ruid-17.html), sur *http://www.centrenational-rfid.com* (version du 13 décembre 2017 sur *Internet Archive*)
30. Jaime Faria, *Les technologies RFID*, techno sans frontière, février 2015 (lire en ligne (http://eduscol.education.fr/sti/sites/eduscol.education.fr.sti/files/ressources/techniques/8397/8397-195-p6.pdf) **[PDF]**)
31. *Tutoriel Tag NFC, Tag RFID* (lire en ligne (https://web.archive.org/web/20170517001348/http://ww2.ac-poitiers.fr/techno/IMG/pdf/tutoriel_nfc_rfid.pdf) **[PDF]**)
32. « Fonctionnement d'un système RFID » (https://web.archive.org/web/20171213054038/http://www.centrenational-rfid.com:80/fonctionnement-dun-systeme-rfid-article-17-fr-ruid-17.html), sur *http://www.centrenational-rfid.com* (version du 13 décembre 2017 sur *Internet Archive*)
33. **(en)** J. Curtin, R. J. Kauffman et F. J. Riggins, « Making the 'most' out of RFID technology: a research agenda for the study of the adoption, usage and impact of RFID », *Information Technology and Management*, Kluwer Academic Publishers Hingham, vol. 8, éditorial 2, 2007, p. 87-110 (ISSN 1385-951X (https://portal.issn.org/resource/issn/1385-951X))
34. Lionel Combes et Jean-Marie Le Bizec, « RFID Démarche de business case pour la supply chain », *Logistique & Management*, vol. 12, 2004, p. 41-48

35. **(en)** Iker Mayordomo, Aritz Ubarretxena, Daniel Valderas, Roc Berenguer et Inigo Gutierrez, « Design and Analysis of a Complete RFID System in the UHF Band Focused on the Backscattering Communication and Reader Architecture », *RFID Systems and Technologies*, VDE, vol. 3rd European Workshop, 2007, p. 1-6 (ISBN 978-3-8007-3045-2)
36. Youssef Bachoti, Bassim Belhaj Sendague et Joao Gabriel Rodrigues Oliveira, *Projet RFID*, janvier 2011 (lire en ligne (https://web.archive.org/web/20171013142926/http://www-public.tem-tsp.eu/~afifi/Rapport%20RFID.pdf) **[PDF]**)
37. « RFID - Radio Frequency IDentification » (https://web.archive.org/web/20071027041933/http://www.guideinformatique.com/fiche-rfid-470.htm), sur *https://www.guideinformatique.com/* (version du 27 octobre 2007 sur *Internet Archive*)
38. « Guide pratique : choisir un tag RFID pour des applications industrielles » (https://web.archive.org/web/20170718005508/https://www.nexess-solutions.com/fr/choisir-un-tag-rfid-pour-des-applications-industrielles/), sur *https://www.nexess-solutions.com/fr/* (version du 18 juillet 2017 sur *Internet Archive*)
39. « Les gammes de fréquences RFID (https://web.archive.org/web/*/http://www.centrenational-rfid.com/les-gammes-de-frequences-rfid-article-16-fr-ruid-17.html) », sur *centrenational-rfid.com* (consulté le 23 juin 2018).
40. Fatima Zahra Marouf, *Etude et conception d'antennes imprimées pour identification radio fréquence RFID UHF* (Thèse d'exercice), Université Abou Bakr Belkaid - Tlemcen, 2013 (lire en ligne (http://dspace.univ-tlemcen.dz/bitstream/112/3813/1/docttl1) **[PDF]**)
41. **(en)** « RFID and Rail: Advanced Tracking Technology - Railway Technology (http://www.railway-technology.com/features/feature1684/) » , sur *railway-technology.com*, 16 mars 2008 (consulté le 14 mars 2018).
42. **(en)** Dipankar Sen, Prosenjit Sen et Anand M. Das, *RFID For Energy and Utility Industries*, PennWell, 2009, 265 p. (ISBN 978-1-59370-105-5, lire en ligne (https://books.google.com/books?id=zSZHbngCGO0C&printsec=frontcover)), pp. 1-48
43. **(en)** Stephen A. Weis, *RFID (Radio Frequency Identification): Principles and Applications*, MIT CSAIL, 2007 (lire en ligne (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.5224))
44. Samuel Fosso Wamba, *Les impacts de la technologie rfid et du réseau epc sur la gestion de la chaîne d'approvisionnement : le cas de l'industrie du commerce de détail* (Thèse d'exercice), Université de Montréal, 2009 (lire en ligne (https://publications.polymtl.ca/147/1/2009_SamuelFossoWamba.pdf) **[PDF]**)
45. Pierre-Henri Thevenon, *Sécurisation de la couche physique des communications sans contact de type RFID et NFC* (Thèse d'exercice), 31 juillet 2012 (lire en ligne (https://tel.archives-ouvertes.fr/tel-00721952) **[PDF]**)
46. Arnaud Vena, *Contribution au développement de la technologie RFID sans puce à haute capacité de codage* (Thèse d'exercice), Université Grenoble-Alpes, 2012 (lire en ligne (https://tel.archives-ouvertes.fr/tel-00922982/document) **[PDF]**)
47. Rafael Antonio Quiroz Moreno, *Solutions novatrices pour l'amélioration du taux de lecture de tags RFID UHF dans des environnements complexes* (Thèse d'exercice), Université Paris-Est, 4 mars 2014 (lire en ligne (https://hal.archives-ouvertes.fr/tel-01133479) **[PDF]**)
48. Mossaab Daiki, *Contribution au développement d'antennes lecteur champ proche pour les systèmes RFID UHF passifs* (Thèse d'exercice), Université Grenoble-Alpes, 2015 (lire en ligne (https://web.archive.org/web/20170812140844/https://www.theses.fr/2015GREAT020.pdf) **[PDF]**)
49. **(en)** « RFID Frequently Asked Question (https://www.rfidjournal.com/faq/show?66) », sur *rfidjournal.com* (consulté le 23 juin 2018).
50. « Identification RFID unitaire, multiple et en aveugle (http://www.centrenational-rfid.com/identification-rfid-unitaire-multiple-et-en-aveugl-article-70-fr-ruid-17.html) », sur *centrenational-rfid.com* (consulté le 23 juin 2018).
51. « Classification des tags RFID » (https://web.archive.org/web/20171227165957/http://www.centrenational-rfid.com/classification-des-tags-rfid-article-19-fr-ruid-17.html), sur *http://www.centrenational-rfid.com* (version du 27 décembre 2017 sur *Internet Archive*)
52. **(en)** Mark Roberti (Founder and Editor), « What Are the Costs of Passive, Active and Semi-passive Tags? (https://www.rfidjournal.com/blogs/experts/entry?10744) » , sur *rfidjournal.com*, 30 septembre 2013 (consulté le 4 janvier 2019).
53. Fabien Humbert, « Les prérequis de la RFID (https://www.lenouveleconomiste.fr/lesdossiers/les-prerequis-de-la-rfid-14167/) » , sur *lenouveleconomiste.fr*, 22 mars 2012 (consulté le 4 janvier 2019).
54. « La RFID : Radio Frequency Identification - Applications logistiques (https://www.faq-logistique.com/RFID.htm) » , sur *faq-logistique.com*, 29 mars 2007 (consulté le 4 janvier 2019).
55. Clotilde Chenevoy, « La RFID révolutionne les magasins Decathlon (https://www.lsa-conso.fr/la-rfid-revolutionne-les-magasins-decathlon,228999) » , sur *lsa-conso.fr*, 13 janvier 2016 (consulté le 4 janvier 2019).
56. **(en)** Edmund W. Schuster, Stuart J. Allen et David L. Brock, *Global RFID : the value of the EPCglobal network for supply chain management*, Berlin/New York, Springer, 2007, 310 p. (ISBN 978-3-540-35655-4, lire en ligne (https://books.google.com/books?id=3547ReFCu9IC&printsec=frontcover))

57. Bernard Jeanne-Beylot, « Les nouvelles générations de tags RFID actifs », *Supply chain magazine*, nº 14, avril 2007 (lire en ligne (http://www.supplychainmagazine.fr/TOUTE-INFO/Archives/SCM014/Tribune-JBeylot-14.pdf))
58. « Identification par radiofréquence (http://iste-editions.fr/products/identification-par-radiofrequence) », sur *iste-editions.fr* (consulté le 18 décembre 2014).
59. **(en)** S. Härmä et V. P. Plessky, « Surface Acoustic Wave RFID Tags », *Development and Implementation of RFID Technology*, février 2009 (ISBN 978-3-902613-54-7, lire en ligne (http://cdn.intechopen.com/pdfs/6032/InTech-Surface_acoustic_wave_rfid_tags.pdf))
60. groupe européen d'éthique des sciences et des nouvelles technologies (2005), Aspects éthiques des implants TIC dans le corps humain**[PDF]** (http://ec.europa.eu/bepa/european-group-ethics/docs/avis20_fr.pdf), Avis du groupe européen d'éthique des sciences et des nouvelles technologies, 39 pages, consulté 2013-03-09.
61. **(en)**Hitachi, *World's smallest and thinnest 0.15 x 0.15 mm, 7.5µm thick RFID IC chip - Enhanced productivity enabled by 1/4 surface area, 1/8th thickness (http://www.hitachi.com/New/cnews/060206.html#top)* (ou version **[PDF]** (http://www.hitachi.com/New/cnews/060206.pdf)) communiqué Tokyo, 2006-02-06, consulté 2013-03-09.
62. Ident Technology (http://www.ident-technology.com).
63. **(en)** Rafael Capurro (Distinguished Researcher in Information Ethics, School of Information Studies, University of Wisconsin-Milwaukee, USA) 2010, *Ethical Aspects of ICT Implants in the Human Body (http://www.capurro.de/wollongong.ppt)* présentation (PPT) faite pour l'IEEE au Symposium on Technology and Society (ISTAS10) University of Wollongong, New South Wales, Australia 7-9 juin 2010.
64. Vidéo du Pr Rafael Capurro lors de l'ISTAS 10 (10e Symposium IEEE sur les technologies et la société) ; conférence "Ethical Aspects of ICT Implants in the Human Body (http://veillance.me/blog/2013/1/22/istas10-ethical-aspects-of-ict-implants-in-the-human-body)", consulté 2013-03-09.
65. « RFID : dangers et dérives des puces sous-cutanées (https://web.archive.org/tech/actualites/technologie-rfid-dangers-derives-puces-sous-cutanees-9090/) »(Archive.org (https://web.archive.org/web/*/https://web.archive.org/tech/actualites/technologie-rfid-dangers-derives-puces-sous-cutanees-9090/) • Wikiwix (https://archive.wikiwix.com/cache/?url=https://web.archive.org/tech/actualites/technologie-rfid-dangers-derives-puces-sous-cutanees-9090/) • Archive.is (https://archive.is/https://web.archive.org/tech/actualites/technologie-rfid-dangers-derives-puces-sous-cutanees-9090/) • Google (https://webcache.googleusercontent.com/search?hl=fr&q=cache:https://web.archive.org/tech/actualites/technologie-rfid-dangers-derives-puces-sous-cutanees-9090/) • Que faire ?), sur *futura-sciences.com* (consulté le 23 juin 2018).
66. « VeriChip : la première puce à implanter dans le corps humain homologuée par la Food And Drug Administration américaine… ou « Big Brother Inside »… (https://atelier.bnpparibas/prospective/article/verichip-premiere-puce-implanter-corps-humain-homologuee-food-drug-administration-americaine-big-brother-inside) » , sur *atelier.bnpparibas*, octobre 2004 (consulté le 4 janvier 2019).
67. **(en)** MAGGIE ASTOR, « Microchip Implants for Employees? One Company Says Yes », *The new york times*, 25 juillet 2017 (lire en ligne (https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html))
68. Dr Fabienne Nsanze (2005), rapport « ICT implants in the human body – A Review », février 2005.
69. Site du GEE (http://ec.europa.eu/bepa/european-group-ethics/index_fr.htm).
70. table ronde intitulée "The ethical aspects of ICT implants in the human body**[PDF]** (http://ec.europa.eu/bepa/european-group-ethics/docs/publications/tb21dec_ict_en.pdf)" du 2004-12-21 (87 pages).
71. Secrétariat du GEE (*Groupe interservice sur l'éthique*) (http://ec.europa.eu/bepa/european-group-ethics/welcome/secretariat/index_fr.htm).
72. BEPA, *Bureau des conseillers de politique européenne (BEPA) (http://ec.europa.eu/bepa/index_fr.htm)* qui se veut être une « passerelle entre les décideurs politiques de la Commission européenne et les acteurs de la société qui peuvent contribuer utilement à l'élaboration des politiques européennes » (groupe organisé sur 2 piliers "*Outreach*" et "*Analyse*", directement placé sous l'autorité du Président de la Commission).
73. Commission européenne, *[1] (http://ec.europa.eu/bepa/european-group-ethics/index_fr.htm)* et mandat 2011-2016 (http://ec.europa.eu/bepa/european-group-ethics/welcome/mandate-2011-2016/index_fr.htm), consulté 2013-03-09.
74. JO C 364 du 18.12.2000, p. 1 à 22, du 28 septembre 2000, approuvée par le Conseil européen de Biarritz (2000-10-14) et proclamée solennellement à Nice par le Parlement, le Conseil et la Commission le 7 décembre 2000.
75. JO L 201 du 31.7.2002, p. 37 à 47.
76. Directive 90/385/CEE du Conseil, du 20 juin 1990, concernant le rapprochement des législations des États-membres relatives aux dispositifs médicaux implantables actifs (JO L 189 du 20.7.1990, p. 17 à 36).
77. Cf. notamment la http://conventions.coe.int/treaty/fr/treaties/html/164.htm Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine], signée le 4 avril 1997 à Oviedo (voir notamment art. 5 à 9 et art. 10).

78. Cf. *Déclaration universelle sur le génome humain et les droits de l'homme (http://portal.unesco.org/shs/fr/ev.php-URL_ID=2228&URL_DO=DO_TOPIC&URL_SECTION=201.html) « Copie archivée » (https://web.archive.org/web/20181108120408/http://portal.unesco.org/shs/fr/ev.php-URL_ID%3D2228%26URL_DO%3DDO_TOPIC%26URL_SECTION%3D201.html#) (version du 8 novembre 2018 sur* Internet Archive*)*, adoptée par l'UNESCO le 11 novembre 1997.
79. *Convention du Conseil de l'Europe, du 1er janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm)*.
80. Cf. point 58 (NTIC) et point 59 (usages abusif des TIC) de la Déclaration de principes du Sommet mondial sur la société de l'information (http://www.itu.int/wsis/) (2003-12-12) sur l'utilisation des technologies de l'information et de la communication (TIC).
81. « Recommandation Européenne 12 mai 2009 (http://www.centrenational-rfid.com/actualites-le-12-mai-2009-la-commission-europeenne-a-adopte-u-fiche-2-fr-ruid-20.html?numPage=1) ».
82. « Site Web de la Cnil - RFID (https://www.cnil.fr/fr/definition/rfid-radio-frequency-identification) ».
83. « Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee) ».
84. « Recommandation de la commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence (https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32009H0387&from=FR) », sur *eur-lex.europa.eu* (consulté le 23 juin 2018).
85. S. MARCELLIN, « Radio-identification : ubiquité, traçabilité et questions juridiques », *Lamy Droit de l'Immatériel, Nº 21*, 1er novembre 2006
86. « Cour de cassation, civile, Chambre sociale, 17 décembre 2014, 13-23.645, Inédit (https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000029941910&fastReqId=1810829239&fastPos=1) » , sur *legifrance.gouv.fr*, 17 décembre 2014 (consulté le 4 janvier 2019).
87. *Conversation d'avenir, la RFID* (http://replay.publicsenat.fr/emissions/conversation-d-avenirs/la-radio-identification/59653), à 13 minutes 20, en replay sur Public Sénat.
88. « le RFID au service d'une gestion rationnelle des déchets (http://www.greenit.fr/article/materiel/recyclage/tagproduct-le-rfid-au-service-d-une-gestion-rationnelle-des-dechets-5268) », sur *greenit.f*, 12 septembre 2014 (consulté le 30 septembre 2014).
89. Recherches RFID portant sur la réduction des ruptures de stock chez Wal-Mart (http://www.radiorfid.com/?p=10), Radio RFID.
90. Advanco (http://www.advanco.com/) et Sanofi, ou IBIZZ (http://www.ibizz.fr/) et Pfizer pour la traçabilité des médicaments.
91. Analogon (http://www.analogon.fr) suivi et maintenance de matériel urbain, jeux publics, arbres d'ornement.
92. DMD Associates (http://www.dmdassociates.com/) spécialiste de l'échange de cartes de visites électroniques par RFID
93. Michaël Torregrossa, « Mondial 2010 - Les bornes de recharge Technolia (http://archive.wikiwix.com/cache/?url=http%3A%2F%2Fwww.avem.fr%2Factualite-mondial-2010-les-bornes-de-recharge-technolia-1778.html) », sur *avem.fr*, 1er octobre 2010.
94. Smart Card Alliance 2003, p. 14
95. « Nice : réglez vos achats avec le service m-carte du Crédit Mutuel - Cityzi.fr (http://www.cityzi.fr/infos/villes/nice/reglez-vos-achats-avec-le-service-m-carte-credit-mutuel) »(Archive.org (https://web.archive.org/web/*/http://www.cityzi.fr/infos/villes/nice/reglez-vos-achats-avec-le-service-m-carte-credit-mutuel) • Wikiwix (https://archive.wikiwix.com/cache/?url=http://www.cityzi.fr/infos/villes/nice/reglez-vos-achats-avec-le-service-m-carte-credit-mutuel) • Archive.is (https://archive.is/http://www.cityzi.fr/infos/villes/nice/reglez-vos-achats-avec-le-service-m-carte-credit-mutuel) • Google (https://webcache.googleusercontent.com/search?hl=fr&q=cache:http://www.cityzi.fr/infos/villes/nice/reglez-vos-achats-avec-le-service-m-carte-credit-mutuel) • Que faire ?), sur *Cityzi.fr*, 5 décembre 2016 (consulté le 27 septembre 2020).
96. Maintag (http://www.maintag.com/) contrôle de la lactation.
97. Jean-Baptiste Waldner, *Nanocomputers & Swarm Intelligence*, Londres, ISTE, 2007, 242 p. (ISBN 978-1-84704-002-2).
98. Céline Le Pichon, « Note méthodologique - Évaluer la fonctionnalité de la Trame bleue pour les poissons », *Sciences Eaux & Territoires*, juin 2017, p. 4 pages (DOI 10.14758/SET-REVUE.2018.25.13 (https://dx.doi.org/10.14758/SET-REVUE.2018.25.13), lire en ligne (http://www.set-revue.fr/note-methodologique-evaluer-la-fonctionnalite-de-la-trame-bleue-pour-les-poissons))
99. Arnaud Caudron, « La technologie RFID pour évaluer le franchissement piscicole d'une buse aménagée de grande dimension », *Sciences Eaux & Territoires*, juin 2020, p. 7 pages (lire en ligne (http://www.set-revue.fr/la-technologie-rfid-pour-evaluer-le-franchissement-piscicole-dune-buse-amenagee-de-grande-dimension))

100. (pt) Mario Cesar Carvalho, « Artista implanta hoje chip no corpo », *Folha de S. Paulo*, 11 novembre 1997 (lire en ligne (https://acervo.folha.com.br/leitor.do?numero=13700&keyword=Kac&anchor=282247&origem=busca&originURL=&pd=e5616b5794dde0ab6a687a693c931980))
101. (es) Luis Esnal, « Un hombre llamado 026109532 », *La Nación*, 15 décembre 1997 (lire en ligne (https://web.archive.org/web/20170201160159/http://www.ekac.org:80/lanacion.html/))
102. (pt) « 1º implante de chip ao vivo - Jornal das 10 - Canal 21 - SP - 1997 (https://www.youtube.com/watch?v=7y2tbPaYqfQ) », 16 janvier 2019 (consulté le 28 juin 2021).
103. (en) Will Weissert, « Microchips implanted in Mexican officials (http://www.nbcnews.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials/) », sur *msnbc.com*, 15 juillet 2004 (consulté le 9 septembre 2019).
104. (en) Raghu Das, « RFID in 2010: The New Dawn (https://www.idtechex.com/research/articles/rfid_in_2010_the_new_dawn_00002437.asp) » , sur *idtechex.com*, 22 juillet 2010 (consulté le 8 août 2018).
105. (en) Raghu Das, « RFID Market in 2012 - up 17% from 2011 (https://www.idtechex.com/research/articles/rfid-market-in-2012-up-17-from-2011-00004585.asp) » , sur *idtechex.com* (consulté le 8 août 2018).
106. (en) Raghu Das et Peter Harrop, « RFID Forecasts, Players and Opportunities 2014-2024 (http://www.centrenational-rfid.com/docs/users/file/RFID_Forecasts_2014_2024.pdf) » , sur *idtechex.com* (consulté le 8 août 2018).
107. (en) Raghu Das, « RAIN RFID 2015-2020: Market size, growth opportunities and trends (http://www.rainrfid.org/wp-content/uploads/2015/07/Das-RAIN_RFID.pdf) » , sur *rainrfid.org* (consulté le 8 août 2018).
108. (en) Raghu Das, « RFID Forecasts, Players and Opportunities 2017-2027 (https://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2017-2027-000546.asp) » , sur *idtechex.com* (consulté le 21 juin 2018).
109. « Taille prévisionnelle du marché mondial pour les étiquettes RFID de 2010 à 2020 (en milliards de dollars des États-Unis) (https://fr.statista.com/statistiques/573542/etiquettes-rfid-previsions-de-la-taille-du-marche-mondial-2010-2020/) », sur *fr.statista.com* (consulté le 21 juin 2018).
110. « Le Marché RFID UHF atteindra 3 milliards de dollars d'ici 2020 » (https://web.archive.org/web/20180621191159/http://www.filrfid.org/2015/07/le-marche-rfid-uhf-atteindra-3-milliard-de-dollars-d-ici-2020.html), sur *http://www.filrfid.org/* (version du 21 juin 2018 sur *Internet Archive*)
111. (en) Raghu Das et Peter Harrop, « RFID Forecasts, Players and Opportunities 2006-2016 (https://www.idtechex.com/research/reports/rfid_forecasts_players_and_opportunities_2006_2016_000137.asp) » , sur *idtechex.com*, octobre 2006 (consulté le 16 juillet 2018).
112. Smart Objects: IBM Global Technology Outlook 2005
113. « 20,1 milliards de radio-étiquettes RFID auront été vendues en 2019, prédit IDTechEx (http://www.lembarque.com/20-1-milliards-de-radio-etiquettes-rfid-auront-ete-vendues-en-2019-predit-idtechex_009304) », sur *lembarque.com* (consulté le 24 juillet 2020).
114. filrfid.org - Vélib et radio-identification (http://www.filrfid.org/article-7008948.html).
115. epcglobalinc.org (http://www.epcglobalinc.org).
116. AFSSET 2008, p. 98.
117. Thomas 2008, p. 1.
118. Dossier futura-sciences. Puce RFID : mythes et réalités du Big Brother miniaturisé - 02/11/2005 (http://www.futura-sciences.com/fr/comprendre/dossiers/doc/t/technologie/d/puce-rfid-mythes-et-realites-du-big-brother-miniaturise_559/c3/221/p1/).
119. van der Togt R, Jan van Lieshout E, Hensbroek R, Beinat E, Binnekade JM, Bakker PJM, *Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment* (http://jama.ama-assn.org/cgi/content/short/299/24/2884), JAMA, 2008;299:2884-2890.
120. Avis de l'Agence française de sécurité sanitaire de l'environnement et du travail [PDF] (http://www.reseaux-telecoms.net/fichiers/dossierpdf/rapport-sur-le-rfid-de-l-afsset.pdf) - AFSSET, 26 janvier 2009.
121. (de) Association allemande FoeBuD pour prévenir les abus potentiels des radio-marqueurs (http://www.foebud.org).
122. Libération/écrans - Interview de Mélanie Rieback (juin 2006) (http://www.ecrans.fr/Il-faut-reflechir-aux-implications.html).
123. Pièces et main d'œuvre - RFID : la police totale [PDF] (http://www.piecesetmaindoeuvre.com/IMG/pdf/RFID_la_police_totale.pdf).
124. L'En Dehors - Vers un contrôle social policier sans faille (http://endehors.org/news/vers-un-controle-social-policier-sans-faille).
125. Annonce de cassage des sécurités de la puce sous-cutanée (http://www.hopenumbersix.net/).
126. VeriChip's human-implatable RFID chips clonable, sez hackers. (https://www.engadget.com/2006/07/24/verichips-human-implatable-rfid-chips-clonable-sez-hackers/) Engadget 24/07/2006.

127. Liste des produits certifiés par l'ANSSI : http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/ « Copie archivée » (https://web.archive.org/web/20120922065633/http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/) (version du 22 septembre 2012 sur *Internet Archive*) Produit certifié : http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2013_08.html

Voir aussi

Sur les autres projets Wikimedia :

Radio-identification (https://commons.wikimedia.org/wiki/Category:RFID?uselang=fr), sur Wikimedia Commons

Bibliographie

- Michel Alberganti, *Sous l'œil des puces, la RFID et la démocratie*, éditions Actes Sud, 2007.
- Philippe Lemoine, « Communication de M. Philippe Lemoine relative à la radio-identification (https://www.cnil.fr/fileadmin/documents/approfondir/rapports/RFID_communication.pdf) »(Archive.org (https://web.archive.org/web/*/http://www.cnil.fr/fileadmin/documents/approfondir/rapports/RFID_communication.pdf) • Wikiwix (https://archive.wikiwix.com/cache/?url=http://www.cnil.fr/fileadmin/documents/approfondir/rapports/RFID_communication.pdf) • Archive.is (https://archive.is/http://www.cnil.fr/fileadmin/documents/approfondir/rapports/RFID_communication.pdf) • Google (https://webcache.googleusercontent.com/search?hl=fr&q=cache:http://www.cnil.fr/fileadmin/documents/approfondir/rapports/RFID_communication.pdf) • Que faire ?) [PDF], sur *cnil.fr*, CNIL, 30 octobre 2003
- Pièces et Main d'Œuvre, *RFID : la police totale*, Editions de L'Échappée, 2008, 80 p.
- Michel Alberganti et Pierre Georget, *La RFID : Quelles menaces, quelles opportunités ?*, Prométhée, coll. « Pour ou contre ? », Bordeaux, 2008 (ISBN 978-2-916623-03-0)
- Étienne Perret, *Identification par radiofréquence : de la RFID à la RFID sans puce*, ISTE Editions, 2014 (ISBN 978-1-78405-055-9)
- AFSSET, *Les systèmes d'identification par radiofréquences (RFID) : Evaluation des impacts sanitaires* (Rapport de l'Afsset 2009 sur les impacts sanitaires), décembre 2008, 1-153 p. (lire en ligne (https://www.anses.fr/sites/default/files/documents/AP2005et0013Ra.pdf) [PDF])
- (en) V.M. Thomas, « Environmental implications of RFID », *International Symposium on Electronics and the Environment, 2008. ISEE 2008. IEEE*, mai 2008, p. 1-5 (ISBN 978-1-4244-2272-2, DOI 10.1109/ISEE.2008.4562916 (https://dx.doi.org/10.1109/ISEE.2008.4562916))
- (en) Smart Card Alliance, *Contactless Payment and the Retail Point of Sale : Applications, Technologies and Transaction Models*, mars 2003, 50 p. (lire en ligne (http://www.it.iitb.ac.in/~tijo/seminar/Contactless_Pmt_Report.pdf) [PDF])

Articles connexes

- ISO/CEI 18000
- Billet électronique
- Communication en champ proche
- Contrôle d'accès
- Contrôle social
- Distance-bounding protocol
- Empreinte environnementale de la RFID
- Exploration de données
- Fichage des populations
- Identité numérique
- Intergiciel pour étiquettes électroniques
- Internet des objets
- Puce sous-cutanée
- Sécurité de l'information au sein des RFIDs
- Système de gestion de cartes à puce

Liens externes

-
-
- Notices dans des dictionnaires ou encyclopédies généralistes : *Store norske leksikon* (https://snl.no/RFID) · *Treccani* (http://www.treccani.it/enciclopedia/rfid)

- Notices d'autorité : GND (http://d-nb.info/gnd/4509863-3) · Tchéquie (http://aut.nkp.cz/ph440131)
- RFID Journal (https://www.rfidjournal.com/)

-