Le droit à la rencontre des technologies de l'information et de la communication: le cas du RFID

Darquennes, Denis; Poullet, Yves; Rouvroy, Antoinette

Published in:
Droit et nanotechnologies

Publication date:
2008

Document Version
le PDF de l'éditeur

Le droit à la rencontre des technologies de l'information et de la communication : le cas du RFID[1]

Yves Poullet
Antoinette Rouvroy
Denis Darquennes

1. L'objectif de la présente contribution est à la fois limité et ambitieux. Il s'agit d'analyser comment la technologie émergente des *Radio Frequency Identifiers* (RFID) s'est développée et comment ses usages se sont régulés dans un premier temps en dehors du droit. Il s'agit ensuite de montrer la manière dont le droit cherche à encadrer cette technologie.

Cette réflexion relative à une technologie particulière s'inscrit dans le contexte plus large des relations entre droit et technologie[2]. Le droit n'est-il pas mis hors jeu par un développement technologique qui, pour n'être pas débattu, en vient à apparaître comme un phénomène naturel et spontané ? Au contraire, l'intervention du droit n'est-elle pas nécessaire précisément pour rendre possible la discussion démocratique à propos des technologies et de leur déploiement, et pour modeler le développement technologique en fonction des exigences sociétales démocratiquement définies ? En retour, le développement technologique n'est-il pas l'occasion, pour le droit, d'approfondir certains de ses présupposés normatifs ?

2. Les RFID présentent, notamment pour le droit, une série d'enjeux spécifiques qui tiennent notamment au fait que cette technologie nouvelle présente une série de caractéristiques inédites : dans la mesure où les RFID, empruntant

1. Notre propos se fonde sur les descriptions et réflexions proposées sur cette technologie par D. DARQUENNES et Y. POULLET, « RFID : Quelques réflexions introductives à un débat de société », RDTI, Janv. 2007, pp. 255 à 285.

2. Sur ces relations entre Droit et Technologie, lire nos réflexions in Mélanges G. HORSMANS, Bruylant, 2004, p. 942 et s. et la thèse de E. LABBE, Les équilibres juridiques à l'épreuve de la contrainte technique, Conflits et défis normatifs de la société de l'information, thèse de doctorat, Université de Montréal, 2 tomes, juin 2006.

aux nanotechnologies, se fondent sur une technologie de l'infiniment petit, l'équipement terminal, c'est-à-dire le microprocesseur qui collecte, traite, émet et/ou reçoit les informations ou les communications externes, peut être d'une taille comparable à celle d'un grain de sable (les *Smart Dusts*). De cette miniaturisation extrême et du fait que les RFID sont des dispositifs de communication « sans contact » naît la possibilité d'interactions largement invisibles entre les « choses » (la souris de l'ordinateur, les marchandises, les vêtements, etc.). L'ensemble de ces applications par lesquelles « *les personnes seront entourées par des interfaces intelligentes et interactives gravées (embedded) dans des objets de tous les jours et un environnement reconnaissant et répondant à la présence d'individus de manière invisible* », constitue ce que l'Union européenne a qualifié d'« *intelligence ambiante* » (*ambient intelligence*)[3]. Cet « *internet des objets* » ouvre des perspectives nouvelles notamment en termes de facilitation des tâches quotidiennes et de surveillance des personnes.

3. Ces technologies ont été conçues au départ dans une perspective plus modeste : il s'agissait de remplacer les codes barres aux capacités de chiffrement réduites et de contourner la nécessité d'un contact physique pour la lecture. Progressivement[4], il est envisagé d'exploiter cette technologie dans d'autres domaines.

La technologie RFID décuple les capacités mémoire du microprocesseur installé sur le produit et, grâce à un dispositif de communication sans contact, permet non seulement une lecture à distance, mais aussi la réaction à des variations de l'environnement, ce qui transforme substantiellement le contrôle et le suivi des produits de leur fabrication jusqu'à leur distribution[5]. Les RFID placées sur les produits facilitent la gestion des stocks, accélèrent le paiement automatique aux caisses, contribuent à la prévention du vol. Placés

3. Le terme est utilisé pour la première fois en 1999 par le Groupe consultatif du programme IST de l'Union européenne (L'ISTAG) dans son rapport sur le futur des technologies. Sur tout cela, J. AHOLA, » Ambient Intelligence », ERCIM News, 2001, n° 47, disponible sur le site : www.ercim.org/publications/Ercim_News/enw47. Cf. également l'expression d'Ubiquitous Computing lancée dès 1991 par M. WEISER, » The computer for the 21st Century », Scientific American, 265 (3), pp. 66 à 75.

4. Sur cette évolution des applications, lire J. BOHM, V. GROAMK, M. LANGHEINRICH, F. MATTERN, M. ROBS, » Living in a World of Smart everyday Objects – Social, Economic and Ethical Implications », Journal of Human and Ecological Risk, 5, Oct.2004, pp. 763-786.

5. Sur ces premières applications et la valeur ajoutée de la technologie RFID par rapport aux codes-barres, lire G.T. FERGUSSON, » Have your Objects call my Objects », Harv. Business Rev., 80 (6), pp. 138-144.

en outre sur le caddie du consommateur ou directement sur la carte shopping de celui-ci, les RFID permettent un « *profilage* » plus subtil du consommateur et de nouvelles stratégies publicitaires. Les tags RFID pourraient aussi permettre une variabilité des prix des produits en fonction d'une série de critères tels que la « *fidélité* » du consommateur, les caractéristiques climatiques du jour, la date de péremption du produit, etc.

Le secteur de la distribution[6] a été le premier à envisager d'utiliser des RFID dans un périmètre initialement limité à la surface des magasins puis débordant progressivement dès lors que des applications « à distance » sont envisagées, telles que le « *frigo intelligent* » qui, sans intervention du consommateur, permettrait de détecter l'absence d'un produit dans le réfrigérateur et de déclencher automatiquement une commande adressée au fournisseur du bien manquant ou à renouveler.

4. Enfin, on peut noter que les « cibles » des applications de la technologie RFID tendent à évoluer : conçues au départ pour « suivre » un produit en ne révélant qu'indirectement, voire involontairement, les comportements et préférences propres aux individus identifiés ou non, ces applications sont de plus en plus utilisées pour « suivre » directement les personnes, les identifier, contrôler leurs comportements, préférences et habitudes. Les RFID peuvent intervenir en renfort des stratégies sécuritaires des autorités publiques.

L'inclusion d'un tag RFID dans les passeports permet ainsi l'identification à distance du porteur. Les RFID peuvent également permettre, dans la perspective du suivi de la clientèle, à la fois de contrôler plus facilement l'accès à certains établissements et d'attribuer « automatiquement » les dépenses et factures aux clients. Dans le contexte des relations de travail, la puce « incorporée » ou simplement « portée par l'employé » permettra à l'employeur de noter les allées et venues des employés. Dans le secteur de l'assurance, l'application de la technologie RFID permettrait de faire varier le montant des primes exigées dans le temps en fonction du comportement de l'assuré[7].

6. Cf. à ce sujet les expériences des chaînes de grands magasins comme Wal-Mart (États-Unis) ou Metro (Allemagne) décrites dans notre article cité note 1.

7. Les questions que poserait l'utilisation éventuelle des RFID dans le contexte de l'assurance, permettant une appréciation de plus en plus fine des différences interpersonnelles actuariellement pertinentes, recoupent partiellement celles qui sont soulevées dans le contexte du débat relatif à la « discrimination génétique » dans l'assurance. À cet égard, voir A. ROUVROY, « Informations génétiques et assurance, discussion critique autour de la position prohibitionniste du législateur belge »,

5. L'imprévisibilité du développement technologique ou plutôt la trajectoire imprévisible des applications d'une innovation technologique conçue au départ dans un objectif précis et débordant rapidement de celui-ci est un phénomène constant dans l'histoire des technologies, mais qui se trouve exacerbé dans le cas de la technologie des RFID[8]. De cette imprévisibilité découle l'impérieuse nécessité d'entourer le développement et le déploiement de cette technologie d'une structure organisée de réflexion permettant à chaque étape de mesurer l'impact social, économique et éthique de la technologie. Si nous plaidons pour une gouvernance de l'internet ayant un tel souci interdisciplinaire, et ce dès la construction de l'objet technologique et de ses premières applications, il importe de retracer la façon dont les marchés de la RFID se sont effectivement organisés pour mettre au point les normes qui régissent le fonctionnement de cette technologie. À cet égard, il apparaît que si le droit a volontiers été mis hors jeu de la régulation de ce marché au profit d'une autorégulation privée et continue à l'être aux États-Unis (I), il entend, en Europe du moins, et ce nonobstant ses lacunes, encadrer progressivement le développement de la technologie (II).

. La gouvernance privée de la technologie RFID

A. L'EPC global – Une étrange similitude avec l'ICANN

6. Les premières applications RFID en matière de logistique exigent par le caractère international des processus qu'elles accompagnent des normes internationales décrivant de manière unique les produits, leurs composants et les entreprises intervenant dans la chaîne logistique.

Un parallèle avec la régulation des noms de domaine et des adresses IP s'impose. On comparera le travail opéré par le consortium « EPC global » avec celui de l'ICANN. Dans un cas comme dans l'autre, il s'agit de garantir une parfaite interopérabilité des applications, en l'occurrence la possibilité pour un lecteur de tag de pouvoir reconnaître et interpréter de manière univoque les données figurant sur le microprocesseur.

7. A l'origine issue de l'association européenne EAN (European Article Numbering) spécialisée dans le codage des produits, l'EPC s'est élargie à la filiale américaine de cette dernière, qui a progressivement pris le leadership et a été rejointe par des structures nationales de normalisation, par des *early adopters* de la technologie comme Gilette, Metro, Wal-Mart, etc., et par les militaires américains, par ailleurs membres du Board of Governors.

On notera le rôle insigne que joue ici, comme à propos du DNS, la société VERSIGN, en établissant un serveur racine des noms d'objets, l'ONS (Object Name Server), serveur auquel se raccrochera l'ensemble des appellations de produits ou éléments.

L'EPC global a établi une collaboration fructueuse avec l'ISO et emprunte volontiers le canal de cette dernière pour donner aux normes dégagées une plus grande visibilité et légitimité. Nous pensons pouvoir à ce stade parler de co-régulation[9], dans la mesure où une institution privée internationale coopère avec une institution internationale publique.

B. Le silence voulu du droit : le cas américain

8. La position américaine privilégie l'autorégulation. Cette solution ne signifie cependant pas l'abstention de toute action et de toute initiative, comme le prouve la mise au point par l'EPC global d'un code de conduite (l'EPC Code) visant à imposer un label et ce, notamment en réaction aux risques d'abus dénoncés par des associations tant de protection des consommateurs (ainsi CASPIAN[10]) que de défense des libertés (ainsi EPIC). L'industrie et le commerce contribuent aussi, par leurs codes de conduite, à apporter une réponse aux risques d'atteinte à la vie privée véhiculés par la technologie RFID, et attestent de la volonté du monde des affaires d'assumer leur responsabilité dans la protection de la vie privée des consommateurs. On cite en

J.T., 16 septembre 2000, pp. 585-603 et A. ROUVROY, Human Genes and Neoliberal Governance : A Foucaldian Critique, Routledge-Cavendish (sous presse).

8. On rapprochera le cas des RFID du cas des cookies qui au départ avaient été prévus pour pallier les risques liés à la déconnexion entre un site et un internaute et qui progressivement ont servi à de multiples applications de profilage individualisé des internautes.

9. Sur la co-régulation, lire nos développements in Y. POULLET, « ICT and Co-regulation : Towards a new regulatory Approach ? », in Starting Points for ICT regulation, B.J. Koops and alii (ed.), T.M.C. Asser Press, ICT & Law 9, 2005, p. 247 et s.

10. Voir le site de CASPIAN et surtout le livre de sa promotrice K. ALBRECHT : K. ALBRECHT and Liz Mc INTYRE, How Major Corporations and Government Plan to Track your Every Move with RFID, Spychips Collection, Penguin, Nelson Current, Oct. 2005.

particulier le *Guide de bonnes pratiques* d'EPC global, rédigé par des experts en vie privée et qui s'applique à tous les membres de l'organisation. Ce guide leur recommande d'adopter différentes actions comme les « *notices* » et l'utilisation de marques, qui permettent d'informer les consommateurs sur la présence de RFID et les usages qui en sont faits. Le guide prévoit la possibilité pour ces derniers d'exercer le choix de bloquer l'identification du tag et rappelle l'obligation de s'assurer du respect de toute législation existante dans le domaine de la protection de la vie privée et des données à caractère personnel.

9. A l'instar des sénateurs du Congrès américain, la Federal Trade Commission, dans ses conclusions d'un atelier (Workshop[11]) réuni en mars 2005, a annoncé qu'elle se contentera de surveiller l'évolution de l'autorégulation en cours, sans publier de directives contraignantes pouvant entraver le développement d'une technologie prometteuse, mais sans toutefois écarter la possibilité d'en édicter dans le futur.

Son argumentation en faveur de l'autorégulation[12] repose sur les arguments suivants : souplesse des solutions rendue nécessaire vu l'évolution des technologies ; primat accordé à la responsabilisation des entreprises et des particuliers ; crainte de la rigidité et de l'inadaptation des solutions réglementaires par définition figées. Le rapport insiste sur les conditions de l'effectivité des solutions proposées par l'autorégulation : éducation et information du consommateur sur les risques et les solutions proposées ; transparence des solutions ; apport de la technologie à l'effectivité des solutions dégagées, etc.

11. RFID : Radio Frequency Identification : Applications and Implications for Consumers ; À Workshop Report from the Staff of the Federal Trade Commission (March 2005) : http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf. Ce workshop réunissait aussi bien les producteurs de RFID, les entreprises utilisatrices que les associations de consommateurs y compris CASPIAN ou des associations de défense des libertés comme EPIC.

12. Sur ces arguments, nos réflexions et références in Y. POULLET, « Les diverses techniques de réglementation de l'internet : l'autorégulation et le rôle du droit étatique », Rev. Ubiquité, 2000, p. 5 et s. Voir aussi P. TRUDEL, « La lex electronica », in Le droit saisi par la mondialisation, (Ch. A. MORAND ed.), Bruxelles, Bruylant, 2001, p. 221.

II. Des relations positives entre le droit et la technologie : l'approche européenne[13]

10. Le monde de la technologie n'est pas en dehors du droit. Le droit, à travers ses concepts et législations existantes, encadre la technologie (A) et ce, au bénéfice d'une sécurité et protection accrue des usagers de celle-ci. C'est ce que nous souhaitons montrer à la fois dans le domaine de la criminalité informatique et de la protection des données.

Il est patent que certaines solutions technologiques peuvent par ailleurs renforcer l'effectivité du droit voire représenter vis-à-vis des prescrits juridiques une véritable valeur ajoutée (B).

Sans doute le droit s'avère-t-il parfois dépassé par la technologie (C), dans la mesure où celle-ci remet en cause certains concepts de droit (le cas de la protection des données est illustratif à cet égard) et peut susciter des interrogations éthiques fondamentales. Le rôle du droit est alors d'organiser le débat sur ces questions afin de définir un encadrement adéquat de ces réalités nouvelles.

A. Le droit encadre

1. La criminalité informatique

11. La Convention européenne sur la cybercriminalité du 23 novembre 2001[14] prévoit un certain nombre de nouvelles infractions dont certaines sont applicables aux radio-tags. En effet, les articles 2 (accès illégal) et 3 (interception illégale) de la section 1 (droit pénal matériel) érigent en infractions pénales d'une part l'accès intentionnel et sans droit à tout ou partie d'un système informatique (dans la mesure où les radio-tags sont considérés comme un système informatique puisque permettant un traitement automatisé de données), et d'autre part l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques (dans la mesure où les données transmises par radio-tag sont des données informatiques).

13. À cet égard, la journée organisée par la Commission européenne sur le RFID et surtout le rapport préparatoire : M. van de VOORT – A. LIGVOET, Towards a RFID Policy for Europe, Workshop Report, 31 Aug. 2006, cité supra.

14. Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 (STE, n° 185).

Ainsi, l'accès aux données contenues dans une puce RFID au moyen d'une borne de lecture placée par une personne non autorisée constitue un *hacking*[15], de même que l'interception non autorisée des données transmises par un RFID à une borne située à distance est punissable. On insiste sur la nécessité tant pour les concepteurs des applications de cette technologie que pour ceux qui les utilisent d'entourer les dispositifs de transmission et les produits RFID d'une sécurité appropriée. Ainsi, le cryptage automatique des transmissions, les contrôles d'accès à la puce, sont autant de mesures que les obligations de sécurité déduites des législations de protection des données imposent. Récemment, à l'occasion de l'utilisation des puces RFID dans les passeports, un débat est mené tant aux États-Unis qu'en Europe sur l'importance de ces mesures de sécurité dans la mesure où, suivant les choix technologiques opérés par les États, la lecture à distance non autorisée des données biométriques et autres contenues dans le passeport s'avère plus ou moins facile[16].

12. Cette application du principe de sécurité affirmé par les lois de protection des données suscite deux réflexions. La première établit clairement que la loi peut poser certaines exigences technologiques: le droit ne se contente pas d'encadrer l'application de la technologie, il peut, comme nous le montrerons plus loin par d'autres exemples, exiger que le design même des systèmes technologiques soit conforme aux prescrits réglementaires. La seconde montre l'importance de l'application de la loi de protection des données et invite à ce sujet à d'autres réflexions.

15. On ajoutera la disposition de l'article 5.3 de la directive 2002/58 CE dite «Protection des données et secteur des communications électroniques», qui interdit de pénétrer dans le terminal sans le consentement de l'utilisateur. Sur cette directive et cette disposition en particulier, lire le commentaire de K. ROSIER, in Concise European IT Law, Kluwer Law Intern., (A. BULLESBACH, Y. POULLET et C. PRIENS éd.), pp.321 et s.

16. À cet égard, les conclusions de la Smart Card Alliance du 3 novembre 2006 (disponible sur le site: http://www.smartcardalliance.org/pages/publications-whti-passport-card) à propos de l'utilisation de la technologie RFID dans les passeports et la possibilité de lire à distance ceux-ci: «the vicinity read Rfid Technology proposed for the passport card, in combination with its weak cryptographic protection, will feed citizen distrust due to the undeniable observation by some technologies that the citizen's unique reference number could be obtained and used to track the citizen whenever the card is outside of its protective sleeve. This raises serious privacy concerns that will have to be overcome if the program is to be embraced by Americans». Dans le même sens, la Déclaration de Budapest sur les documents de voyage à lecture automatique (MRTD-Machine Readable Travel Documents) disponible sur le site de la FIDIS (projet de recherche européen): http://www.fidis.net/press-events/press-releases/declaration-de-budapest:

2. L'application des lois de protection des données

13. La technologie RFID constitue un défi nouveau et sans précédent pour la protection de la vie privée dans la mesure où elle remet en cause les «*frontières naturelles*»[17], celles sur lesquelles tout citoyen compte naturellement pour protéger son intimité et sur lesquelles il fonde ses attentes légitimes en matière de protection de sa vie privée: frontières physiques, dans la mesure où les RFID pénètrent nos murs, nos portes, nos poches; frontières sociales dans la mesure où nous nous reposons sur la confiance que nous pouvons avoir dans certains groupes sociaux comme les médecins, alors même que les systèmes RFID ouvrent ces cercles de confiance à des tiers que nous ignorons; frontières temporelles et spatiales qui créent des barrières entre les différents moments de notre vie, abolies aujourd'hui par un fait technologique qui permet le rappel et le croisement indéfinis de faits survenus en des lieux divers et en des temps différents; frontières enfin dues au caractère éphémère et purement transitoire d'événements dont nous espérons l'oubli immédiat: l'hésitation devant une marchandise ou une vitrine, à jamais fixée grâce à une technologie qui autorise une surveillance de tous les instants et agit comme une «*mémoire amplifiante*»[18].

14. Dans les cas où la directive 95/46/EC trouve à s'appliquer – et nous verrons que ce n'est pas toujours nécessairement le cas – les responsables du traitement (c'est-à-dire ceux qui utilisent les données collectées grâce aux RFID) sont tenus de respecter les obligations qui en découlent[19].

Ils doivent s'assurer que les données qu'ils traitent le sont loyalement et licitement: ils doivent informer, de façon claire et compréhensible, les

17. Voir G.T. MARX, «Murky Conceptual Waters: the Public and Private Ethics and Information Technology», cité par J. BOHM, V. CUROAMD et alii, art. cité supra note 1.

18. R.N. MAYO, «The Factoids Project», article disponible sur le site http://www.research.compaq.com/wrl/techreports/abstracts/TN-60.html.

19. Il est intéressant de noter que les prescrits légaux peuvent être prolongés par des codes de conduite ou autres formes de régulation moins contraignantes mais plus précises telles que les Privacy Guidelines for the RFID Information Systems publiées par l'Information and Privacy Commissioner de l'Ontario, qui traduisent en un texte à l'attention des designers et des users de la technologie RFID les conséquences de l'application des lois de protection des données au développement et au déploiement des applications RFID. (Ces RFID Privacy Guidelines de juin 2006 sont accessibles sur le site de la Commission de l'Ontario: (http://www.ipc.on.ca). On peut songer à des codes ou des labels spontanément mis en place par les entreprises elles-mêmes. Bref, l'autorégulation peut prolonger l'œuvre du droit.

personnes concernées par l'utilisation de ces technologies de la présence de dispositifs RFID. Ils doivent informer les personnes concernées, au minimum, de l'identité du responsable du traitement, des finalités du traitement auquel les données sont destinées, des destinataires des données et de l'existence d'un droit d'accès et de rectification des données conservées. Dans le cas du commerce de détail, cela se traduit par l'obligation de mentionner, outre le marquage des produits par des radio-tags, leurs finalités et la présence de lecteurs, le fait que cette lecture peut s'opérer indépendamment de la volonté de la personne et la possibilité de désactivation par cette dernière[20].

Les données recueillies doivent être pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Par ailleurs, elles doivent être exactes et, si nécessaires, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. Les responsables du traitement doivent s'assurer que les données sont collectées pour des finalités déterminées, explicites et légitimes et ne seront pas traitées ultérieurement de manière incompatible avec ces finalités. Les données permettant l'identification des personnes concernées ne peuvent d'ailleurs pas être conservées au-delà de la durée nécessaire à la finalité du traitement ou conservées sous une forme permettant l'identification des personnes concernées.

En ce qui concerne la légitimité des traitements opérés à partir de l'utilisation des RFID, le Groupe de l'article 29 souligne qu'en principe le consentement préalable des individus[21] est toujours nécessaire à la légitimité du traitement. Ce consentement ne devrait être considéré comme valide, à notre avis et sauf exception[22], que dans la mesure où il se fonderait sur une information claire à propos de l'existence, du type, de la localisation, des finalités et

20. Le parallèle avec le droit de restreindre l'identification de la ligne appelante et de la ligne connectée, droit consacré par l'article 8 de la Directive 2002/58, peut être proposé à ce propos. On note que cet article oblige le fournisseur du service de communication à offrir à l'abonné un moyen simple et gratuit d'empêcher la présentation de l'identification de la ligne appelante, de refuser des appels entrants de lignes non identifiées, ou de la présentation de l'identification de la ligne connectée.

21. Il faut préciser que dans le cas du consentement donné, ce dernier doit respecter certaines exigences: il doit être donné librement (sans contrainte ou tromperie), être spécifique (c.à.d. concerner une finalité particulière), être une indication de la volonté effective de la personne, et finalement être donné en toute connaissance de cause et être indubitable (c.à.d. qu'il ne peut avoir plusieurs sens).

22. Ainsi, moyennant le respect du principe de proportionnalité, dans le cas d'intérêt public

des actions rendues possibles par la technologie RFID de même qu'à propos de la nature des informations transmises et de l'identité de leurs destinataires. Le consentement doit en outre être rétractable, ce qui implique la possibilité de désactiver momentanément ou définitivement le radio-tag, ce qui impose certaines contraintes pour la technologie des microprocesseurs à mettre en place.

15. Le respect de ces obligations sera facilité s'ils disposent d'une technologie qui, dès sa conception par les fabricants, incorpore les moyens techniques permettant de respecter les exigences légales. Voilà qui met en évidence la part de responsabilité des fabricants vis-à-vis du principe général du respect de la vie privée. Cette responsabilité se déduit du considérant 2 de la directive 95/46: «*les systèmes de traitement sont au service de l'homme... doivent respecter les libertés et droits fondamentaux des personnes, notamment la vie privée... doivent contribuer au progrès économique et social et au bien-être des individus*». L'article 14 alinéa 3 de la directive 2002/58 donne à ce principe de responsabilité des fabricants une première concrétisation lorsqu'elle affirme: «*Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel...*».

B. La technologie au secours du Droit

16. L'apport technique à la garantie du respect de tels prescrits s'opère sur différents plans selon le Groupe de l'article 29[23]: normes techniques relatives à l'interopérabilité des éléments de la technologie RFID; mesures techniques et d'organisation informant sur la présence de RFID, leur visibilité, leur état de veille, et permettant également leur neutralisation temporaire – mécanique ou par brouillage logiciel – ou permanente – au moyen d'une commande de destruction (commande *kill switch*), d'un brouillage de mémoire ou d'un détachement mécanique du tag; mesures techniques et d'organisation pour l'exercice des droits d'accès, de rectification et d'effacement des données; implantation de dispositifs de neutralisation autorisant la personne à retirer à tout moment son consentement; sécurisation des données via des mesures

dûment justifié comme le cas des passeports munis d'un RFID ou d'intérêt vital du patient dans un hôpital.

23. Les références aux articles contenues ci-après sont des références à la Directive 95/46/CE. Les exemples sont souvent repris de l'article déjà cité: D. DARQUENNES-Y. POULLET, cité supra, note 1.

techniques – telles que des protocoles d'encryptage, ou la mise au point de *blocker tags* interdisant la communication avec un lecteur non autorisé.

C. Le droit dépassé par la technologie

17. Nonobstant la clarté apparente des droits et obligations consacrés par la Directive 95/46/CE, force est de constater que la technologie RFID défie les dispositifs juridiques de protection des données à caractère personnel, et ce à plusieurs titres[24].

Si l'on perçoit bien en quoi le déploiement des RFID dans les espaces tant privés que publics peut frustrer, si l'on n'y prend garde, les attentes légitimes des citoyens relativement à la protection de leur vie privée, il ne va pas pour autant de soi que les applications RFID tombent nécessairement dans le champ d'application des lois de protection des «*données à caractère personnel*», comme en témoignent notamment les doutes émis par le «Groupe dit de l'article 29» à cet égard. La particularité des RFID consiste dans le fait qu'elles introduisent un lien entre un objet et des informations relatives à cet objet (sa chaleur, sa localisation, etc.), cet objet fût-il le corps lui-même. Sans doute, et c'est le but, peut-on à partir de là inférer des informations relatives au possesseur de l'objet ou à celui qui le porte et déclencher certaines actions curatives, publicitaires ou autres vis-à-vis de lui. Pour autant, il n'est pas nécessaire de connaître son identité ni même de la rechercher. Ce qui importe est que le sujet X, porteur du RFID, se trouve à tel endroit, a fait tel achat, est en possession d'un titre de transport valable, et ce afin de déclencher vis-à-vis de lui l'action appropriée.

Peut-on à ce propos parler de données à caractère personnel, au sens de l'article 2 a) de la directive 1995/46/CE? La notion d'identité est au cœur de la définition de ce type de données. Sans doute cette définition est-elle large, dans la mesure où, comme le rappelle le groupe de l'article 29 à propos des cookies ou des RFID, en invoquant le considérant 26, l'«*identifiabilité*» se conçoit en fonction de «*l'ensemble des moyens susceptibles d'être raisonnablement mis en place, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne*». Outre que comme le reconnaît le groupe lui-même,

24. Voir à cet égard le document de travail du «Groupe 29» sur les questions de protection des données posées par la technologie RFID, document du 19 janvier 2005 WP n° 105, disponible sur le site de la Commission: http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr. pdf

cette approche, même large, de la notion de données à caractère personnel ne permet pas de couvrir tous les cas, elle reste théorique dans la mesure où ceux qui exploitent les données nées des cookies[25] ou des RFID[26] ne cherchent pas à identifier la personne concernée mais simplement à profiler[27] le détenteur d'un terminal pour décider vis-à -vis de lui de certaines actions. Sur ce point, la réponse à la question de l'application de la directive sera à donner pour chaque application de la technologie RFID, après examen au cas par cas de la présence ou non d'un traitement de données à caractère personnel, tel que défini par la directive générale *Protection des données à caractère personnel*. Tout utilisateur des informations collectées au moyen de la technologie RFID devra donc au préalable évaluer si cette dernière est effectivement considérée comme «*donnée à caractère personnel*». En fait, si l'information du radio-tag ne contient aucun renseignement personnel et n'est pas non plus combinée avec des données à caractère personnel, alors la directive protection des données ne s'appliquera pas, comme l'a souligné le Groupe 29.

18. En d'autres termes, les données générées par les RFID ne sont pas nécessairement des données à caractère personnel. Peut-être une autre définition de la donnée à caractère personnel est-elle nécessaire, fondée cette fois sur la notion de «*contactabilité*»[28], c'est-à-dire le fait que des données permettent ou non de contacter un individu, d'influencer son comportement ou de

25. Dans le cadre des cookies, les données générées par les cookies se réfèrent à un terminal et une adresse IP et non à l'individu possesseur du terminal ou de l'adresse IP. Le rapprochement avec le cas des RFID est intéressant dans la mesure où les personnes qui bénéficient des données générées par les cookies n'ont de même aucun besoin de connaître l'identité de la personne concernée.

26. Document de travail, déjà cité en date du 19 janvier 2005.

27. Cette notion de profilage pourrait conduire à considérer que la recherche de l'identité s'opère alors par référence non à des données administratives (nom, prénom, adresse, etc.) mais par rapport «à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale», comme le permettrait le dernier membre de phrase de l'article 2 a) de la directive. Ainsi, un cookie générerait des données à caractère personnel lorsque le nombre de données collectées grâce au cookie permettrait de constituer une image suffisamment précise de la personnalité de l'individu, peu importe l'aspect considéré (profil économique, psychologique ou physiologique). Cette piste apparaît plus féconde mais elle se heurte au fait que dans l'esprit de la directive, ces profils ne sont pas pris pour eux-mêmes et ne constituent des données à caractère personnel que dans la mesure où ils permettent de découvrir l'identité de la personne concernée.

28. Sur ce critère, les réflexions de Y. POULLET et J.M. DINANT in «Information Self-determination in the Internet area», Report on the application of data Protection principles to the worldwide telecommunications networks, Consultative Committee of the Convention for the protection of indi-

prendre une décision vis-à-vis de lui mais en l'état actuel du droit ce critère n'est pas retenu[29]. Sans doute la protection des droits et libertés individuels dans un univers truffé de RFID nécessitera-t-elle quelques innovations dans le champ du droit. Aussi faut-il, dans une perspective prospective des enjeux sociétaux induits par les RFID, développer des notions nouvelles pour décrire ce qui devrait faire l'objet d'une protection juridique, au-delà de la simple protection des données à caractère personnel.

À titre d'exemple, suggérons le principe d'*attentional privacy*, dont on pourrait argumenter qu'il est une application du droit à la protection de la vie privée et familiale garanti à l'article 8 de la Convention européenne des droits de l'homme (dans la mesure notamment où il permettrait de protéger la personne, dans sa sphère privée, contre des actes de harcèlement épistolaire[30]), recouperait partiellement les prérogatives qui résulteraient pour l'individu de la reconnaissance de la «*contactabilité*» comme critère définissant les données à caractère personnel.

L'on pourrait aussi utilement explorer les mérites du principe d'«*intégrité contextuelle*» avancé par Helen Nissenbaum[31] et inspiré de la théorie des «*sphères de justice*» de M. Walzer[32], qui interdirait que des informations personnelles recueillies et communiquées dans un contexte déterminé (par exemple la sphère familiale, le club de sport, l'emploi, les soins de santé, «*microcosmes sociaux relativement autonomes*»[33]) dans lequel les flux informationnels obéissent aux «*lois*» spécifiques à ce contexte (on ne «*communique*» pas de la même façon dans le cercle de la famille et dans le cercle professionnel), puissent être recueillies et communiquées dans des contextes différents, régis par d'autres «*lois*».

viduals with regard to automatic processing of personal data, Strasbourg 13/12/2004, T-PD (2004) 04 final. En ligne sur le site du Conseil de l'Europe.

29. Dans un autre écrit (Y. POULLET, «Pour une troisième génération de législations de protection des données», JusLetter, n° 3, October 2005), nous avons essayé de montrer combien la directive 2002/58 lorsqu'elle réglemente les données de trafic et de localisation générées par l'utilisation des services de communication se soucie peu du fait que ces données soient des données à caractère personnel.

30. Voir par exemple l'arrêt de la Cour suprême du Tennessee, Moorhead v. J.C. Penney Company, Inc., 555 S.W. 2d 713 1977, cité par F. RIGAUX, La protection de la vie privée et les autres biens de la personnalité, Bruylant, 1990, p. 324.

31. H. NISSENBAUM,» Privacy as Contextual Integrity», Washington Law Review, 2004, 119-158.

32. M. WALZER, Spheres of Justice: A Defense of Pluralism and Equality, Basic Books, 1983.

33. P. BOURDIEU, Réponses. Pour une anthropologie réflexive, Seuil, 1992, p. 72.

Les ressources imaginatives du droit seront aussi probablement sollicitées pour adapter les réglementations en vigueur afin de préserver la «*texture*» des vies individuelles face aux nouvelles vulnérabilités. Peut-être faudra-t-il à ce titre combler l'écart qui pourrait se creuser entre la conception juridique actuelle des données sensibles – que l'article 8 de la Directive 95/46/CE définit comme des données à caractère personnel, celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou sont relatives à la santé et à la vie sexuelle – et les perceptions sociales de ce que seraient des données sensibles dans un monde où les possibilités techniques offertes par les RFID permettraient des intrusions nouvelles dans l'intimité des rapports interpersonnels dans les lieux publics et privés. Il est probable que des informations relatives à la qualité de certaines interactions sociales dans des lieux publics soient perçues par ceux qui y sont impliqués comme particulièrement sensibles, de même que certaines informations relatives à leur localisation, ne fût-ce que dans la mesure où ces informations révèlent indirectement leurs opinions politiques, convictions religieuses, leur santé ou leur vie sexuelle, ou parce qu'elles relèvent d'activités que les personnes impliquées ne souhaitent pas faire connaître à leur entourage (on retrouve ici la notion d'intégrité contextuelle).

Par ailleurs, l'idée est suggérée depuis un certain temps dans la littérature féministe et post-structuraliste que la «*personne*», le sujet digne de la protection du droit, ne serait plus réductible au sujet situé spatialement et circonscrit physiquement[34]. Les «*échantillons informationnels*» désincarnés rassemblés dans des banques de données, dans cette optique, constituent des «*identités informationnelles*»[35] parallèles et donc séparées mais entretenant un réseau d'interactions avec le sujet incarné et avec la biographie personnelle à travers laquelle l'individu construit et maintient la perception qu'il a de lui-même. Pourrait-on concevoir dès lors que la Directive 95/46/CE puisse être applicable plus généralement aux informations recueillies grâce à la technologie RFID dès lors qu'elles se rapporteraient à une «*personne informationnelle*», à l'«*identité virtuelle*» d'une personne physique, sans que la personne physique elle-même doive être identifiable?

34. Harraway, notamment, avait développé, à l'égard du développement de la génétique humaine, un raisonnement assez proche. Voir notamment D.J. HARRAWAY Modest_Witness@Second_Millenium. FemaleMan_Meets_OncoMouse: Feminism and Technoscience, Routledge, 1997.

35. Voir K.F. AAS, «The Body Does Not Lie: Identity, Risk and Trust in Technoculture», Crime, Media, Culture, 2: 143-158.

Le privilège conféré aux identités «*informationnelles*» par rapport aux identités «*autobiographiques*», notamment dans le contexte d'opérations de «*profilage*» que faciliteraient les RFID, n'est pas sans conséquence: invalider les récits individuels qui sous-tendraient des demandes d'accès à certaines prestations et services, notamment dans le secteur social et des soins de santé, pour leur préférer des informations récoltées par le biais des RFID et/ou du profilage risque d'accroître la vulnérabilité de sous-populations déjà fragilisées, les privant de leur «voix», seul média par lequel elles peuvent témoigner des difficultés de leur situation et tenter d'infléchir les algorithmes de décisions qui leur sont appliqués. Dans cette perspective, l'on perçoit que les enjeux des RFID ne sont pas limités à la protection des données mais impliquent potentiellement des valeurs plus larges et requièrent la mise en œuvre d'un débat éthique fondamental.

19. La technologie RFID révèle donc l'insuffisance du droit de la protection des données à caractère personnel face à la perspective des risques pour la vie privée qu'induirait le déploiement massif de la technologie RFID. Face à ce décalage entre le droit positif et l'ampleur des défis nouveaux, le droit n'a d'autre alternative que de mettre en place les conditions d'un débat démocratique à propos du développement de la technologie RFID, de son déploiement, et de ses applications. Dans la mesure où un débat démocratique véritable nécessite un degré d'autonomie suffisant des personnes qui y participent, il revient au droit de garantir les conditions d'existence et d'exercice de cette autonomie. Il paraît important à cet égard d'explorer différents scénarios possibles d'une société dans laquelle les RFID seraient largement répandus, et de voir quelles sont les conditions à mettre en place pour éviter que la présence de cet «*internet des objets*» n'interfère avec l'autonomie des individus, avec leur capacité à faire des choix réellement libres. Les nouvelles technologies publicitaires, par exemple, sous prétexte d'information du consommateur, peuvent constituer une menace pour l'intégrité des choix individuels et, partant, porter atteinte à l'autonomie de l'individu.

Le principe fondamental du consentement individuel, libre et informé, qui doit pouvoir être retiré à tout moment, relève de cette exigence de protéger l'autonomie individuelle. La question de savoir si le consentement seul suffit à conférer une justification à toute intervention intrusive vis-à-vis de l'intégrité physique, question fort débattue dans le champ de la philosophie politique notamment, pourrait se poser également à l'égard des interventions intrusives vis-à-vis de l'intégrité informationnelle, et ceci d'autant plus que le consentement d'un individu au traitement de ses informations personnelles peut, indirectement, dans la mesure où ce consentement lui garantit un avantage comparatif en terme d'employabilité, d'assurabilité, ou simplement de prime ou de cadeau publicitaire, désavantager ceux qui seraient moins enclins à «*échanger*» leurs informations personnelles contre ces divers bénéfices, avantages, services ou commodités.

Dans cette perspective, l'on perçoit que les enjeux des RFID ne sont pas limités à la protection des données mais impliquent potentiellement des valeurs plus larges, et requièrent la mise en œuvre d'un débat éthique fondamental.

Conclusions

20. Le débat sur les RFID illustre le difficile dialogue entre droit et technologie. Saisi par une technologie galopante et à la recherche de ses applications, le droit hésite à s'affirmer. Le fait économique, voire politique, qui se cache derrière le soi-disant diktat technologique, lui enjoint le laisser-faire. Sans doute le réveil du droit sonne au moment où la technologie montre ses propres dérives. Sans doute son intervention est-elle jugée alors tardive, souvent timide, parfois brutale. Sans doute l'effectivité de cette intervention suppose-t-elle d'autres concours, à savoir celui des milieux intéressés eux-mêmes, de la technologie elle-même surtout.

Peut-être doit-on prendre conscience du fait que l'idée même d'un fait technologique est fausse, que tout depuis le début est affaire de choix? Instaurer la nécessité d'une réflexion sur ces choix, n'est-ce pas le premier rôle du droit? Au terme de notre réflexion, nous plaidons pour un droit qui ait perdu de sa superbe: celui de dicter les choix; nous plaidons pour un droit qui simplement modestement crée les conditions de ces choix technologiques, un droit qui institue le débat au cœur du développement technologique. Il n'y a pas lieu d'imposer, il y a lieu de réfléchir ensemble sur ce que nous souhaitons d'une technologie au service de l'Homme, de sa dignité et de ses libertés, de poser les conditions du dialogue entre toutes les parties intéressées: les promoteurs de ces technologies, les responsables des applications, les consommateurs, les patients, les défenseurs des libertés, et espérer au terme de ces discussions une solution que le droit alors relaiera avec le concours de chacun, technologie y comprise.

Enfin, peut-être faudrait-il aussi prendre conscience du fait que beaucoup des nouvelles menaces pour la vie privée doivent être comprises

«*architecturalement*», en tant qu'elles participent d'une structure sociale et juridique plus large, d'une configuration particulière de notre organisation sociale et économique. Il s'ensuit qu'il est insuffisant, pour protéger la vie privée à l'ère des RFID, de se focaliser seulement sur la réparation et les sanctions d'infractions particulières au droit à la protection des données à caractère personnel, mais qu'il est aussi, fondamentalement, nécessaire d'établir une structure sociale qui assure de fait que les individus revendiqueront bien l'exercice de leurs droits, et que les responsables des traitements de données rempliront effectivement leurs obligations en matière de protection de la vie privée.