la lettre EMERIT

Expériences de Médiation et d'Évaluation dans la Recherche et l'Innovation Technologique

Trimestriel d'information sur l'évaluation des choix technologiques, édité par la Fondation Travail-Université

Quatrième trimestre 2006
Numéro 48

Bureau de dépôt: Namur 1
Numéro d'agréation P401118

Les enjeux sociétaux des technologies convergentes

L'expression "technologies convergentes" désigne la rencontre, peu fortuite, d'innovations dans les domaines de la microélectronique, de la bioinformatique, des nanotechnologies et des sciences cognitives. Quelques objets, qui commencent à devenir familiers, illustrent cette convergence: les étiquettes émettrices de radiofréquences (RFID), les puces biométriques dans les passeports, les implants électroniques dans le corps humain. La technologie avance aux frontières de la connaissance scientifique, sous la pression de puissants intérêts commerciaux ou politiques, parfois spéculatifs.

Ce numéro spécial de la Lettre EMERIT traite des enjeux sociétaux et éthiques soulevés par les technologies convergentes. Il fait référence à des travaux récents d'institutions scientifiques et à des initiatives de débat public. Avec un mot clé: anticiper.

Selon la Commission européenne, les technologies convergentes sont "des technologies et des systèmes de connaissance génériques qui se renforcent mutuellement dans un objectif commun". Pour comprendre cette définition, il faut se référer aux quatre familles de technologies qui sous-tendent la convergence: les nanotechnologies, les biotechnologies, les technologies de l'information et de la communication et les sciences cognitives (voir l'encadré de la page suivante). L'abréviation NBIC (nano, bio, info, cognitive) est souvent utilisée pour caractériser cette convergence.

Des approches prudentes de la convergence

Aux États-Unis, la National Science Foundation souligne que l'objectif à long terme de la convergence NBIC ne concerne pas tant la maîtrise de la matière que la possibilité de modifier les capacités physiques et intellectuelles des êtres humains. Elle a mis en place un programme de recherche pluriannuel intitulé "Convergence NBIC pour l'amélioration des performances humaines".

En Europe, les orientations des politiques de recherche semblent à la fois plus prudentes et mieux ancrées dans un projet de développement économique et social, sans prendre nécessairement pour objectif la modification des performances humaines. En outre, elles visent à anticiper à la fois les avantages et les risques pour l'économie et pour la société.

C'est ainsi que la Commission européenne a soutenu un exercice de prospective technologique, piloté par

Numéro spécial *Technologies convergentes*

Depuis 2006, la Lettre EMERIT est publiée avec le soutien financier du Fonds National de la Recherche Scientifique (FNRS)

un groupe d'experts, qui a débouché en 2005 sur la proposition d'une démarche spécifiquement européenne, intitulée "Technologies convergentes pour la société de la connaissance".

Les grandes lignes de l'approche européenne

Le rapport Nordmann propose une vision des technologies convergentes et de leurs impacts sur la société, qui repose sur quatre piliers:

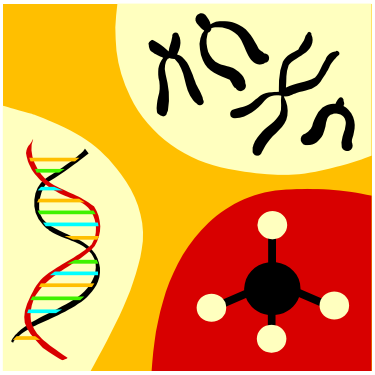
– Développer une vision à long terme et une stratégie pour introduire la convergence technologique dans les programmes de recherche thématiques sur les nanosciences, les sciences du vivant, les TIC, les neurosciences et les sciences humaines et sociales, notamment en créant des réseaux d'excellence européens.

– Formuler de nouveaux agendas de recherche, qui favorisent les approches interdisciplinaires, notamment l'interaction entre les sciences de la matière, les sciences du vivant et les sciences humaines.

– Développer une structure d'encadrement de la recherche sur les technologies convergentes: normalisation technique, cadre juridique, code de bonne conduite, observatoire social chargé d'une évaluation sociétale continue des projets et des réalisations.

– Mettre en place un modèle de gouvernance des technologies convergentes, qui repose sur des processus de décision transparents; une implication des comités nationaux et européens d'éthique des sciences et des technologies; un système adéquat de propriété intellectuelle; des débats publics nationaux favorisant l'expression des points de vue et intérêts en présence.

Dans la pratique, de nombreux projets de technologies convergentes ne couvrent pas tous les domaines de la "convergence NBIC", ils ont des objectifs moins ambitieux et plus pragmatiques, qui visent à créer un consensus dans la société plutôt qu'à susciter des controverses. La convergence technologique peut apporter des solutions concrètes à des problèmes de régulation énergétique, de surveillance environnementale, de gestion des systèmes de transport, de diagnostic médical, de prothèses, d'outils techniques pour faire face à des handicaps, et d'autres encore. Cette orientation vers la résolution de problèmes d'intérêt général est une des spécificités de l'approche européenne de la convergence technologique.



Les travaux du Groupe européen d'éthique des sciences et des technologies (GEE) vont dans le même sens. Ils soulignent la nécessité d'examiner systématiquement les opportunités et les risques de technologies qui s'aventurent à la fois aux frontières de la connaissance et aux frontières de l'éthique, notamment lorsqu'il s'agit d'artefacts destinés à modifier, programmer ou contrôler des comportements humains.

Anticipation, débat public et gouvernance

Trois thèmes communs traversent les deux rapports cités dans cet article: l'anticipation, le débat public et la gouvernance.

Tirant les leçons des nombreuses controverses suscitées a posteriori par le développement des biotechnologies, jugé trop technocentrique, les

La convergence "nano bio info cognitive" (NBIC)

Les *nanotechnologies* permettent de manipuler la matière et de construire de nouvelles structures à l'échelle du millionième de millimètre (nanomètre), c'est-à-dire la taille de quelques atomes ou molécules. Elles ouvrent la voie non seulement à la fabrication de matériaux nouveaux, mais aussi à des applications biologiques, médicales et pharmaceutiques, notamment à travers des implants artificiels dans le corps humain.

Les *biotechnologies* visent à une connaissance détaillée du fonctionnement des gènes et des cellules vivantes, ainsi que des processus qui peuvent conduire à des maladies ou des pathologies. Alliées à l'informatique, elles conduisent à une modélisation de ces processus biologiques. Alliées aux nanotechnologies et à la microélectronique, elles peuvent mener à des applications de diagnostic au niveau cellulaire, à des capteurs électroniques à l'échelle moléculaire, à des systèmes de dosage de molécules pharmaceutiques intégrés dans des organes et commandés à distance.

Les *technologies de l'information et de la communication* (TIC) permettent d'organiser la communication entre des "micropuces" ou "nanopuces", c'est-à-dire des processeurs miniaturisés à l'échelle micrométrique ou nanométrique, et des systèmes informatiques situés dans leur environnement. Elles évoluent vers un "internet des objets communicants". Quant à l'intelligence artificielle, elle se situe aux confins de l'informatique et des sciences cognitives.

Les *sciences cognitives* visent à une modélisation des processus de perception, de diagnostic et d'interaction; elles s'adressent aussi aux interfaces entre les êtres humains et les artefacts technologiques. Elles s'articulent aux neurosciences et à d'autres disciplines des sciences humaines, comme les théories du comportement, la sémiotique, les théories de la représentation et de la communication. Alliées aux TIC et aux nanotechnologies, elles s'orientent vers la conception de systèmes sensorimoteurs ou cognitifs qui intègrent les interactions d'éléments humains et non humains.

auteurs souhaitent traiter les questions d'éthique et d'acceptabilité sociale dès la conception des programmes de recherche, en amont des applications technologiques. Cette stratégie d'anticipation vise à sélectionner des domaines de développement technologique qui optimiseront l'efficacité économique et l'utilité sociale des technologies convergentes.

Lorsque des technologies s'aventurent à la fois aux frontières de la connaissance et de l'éthique, les opportunités et les risques doivent faire l'objet d'une évaluation systématique, continue et transparente.

Le débat public devient dès lors incontournable. Il s'agit d'ouvrir la réflexion sur les technologies convergentes à toutes les parties concernées, d'assumer les controverses et de rendre les décisions transparentes pour l'opinion publique. Une des conséquences du débat public est que, dans un cadre européen commun, les orientations choisies par différents pays puissent refléter des spécificités culturelles ou sociales, ou des priorités particulières en termes de santé ou de bien-être.

Enfin, l'insistance sur les questions de gouvernance révèle un souci de ne pas laisser le développement des technologies convergentes s'aligner sur les seules logiques de rentabilité économique, de compétitivité et de mondialisation des échanges. Est-ce un retour aux sources de la notion de politique de R&D ?

- Nordmann A. (éd.), *Technologies convergentes – façonner l'avenir des sociétés européennes*, Rapport du groupe d'experts de haut niveau, Commission européenne, EUR21357-FR, 2005.
- Groupe européen d'éthique des sciences et des nouvelles technologies, *Rapport d'activités 2000-2005*, Commission européenne, Luxembourg, 2005.

RFID, l'étiquette communicante

Tags, étiquettes communicantes, puces à radiofréquence, tous ces termes désignent des dispositifs d'identification à radiofréquence (*RFID, radiofrequency identification device*). Ces nouveaux objets techniques consistent en une puce munie d'un processeur, d'une mémoire et d'un émetteur radio. Souvent miniaturisés, les dispositifs RFID sont destinés à s'intégrer dans d'autres objets ou dans des êtres vivants, pour interagir avec leur environnement. Quatre grandes catégories d'usages peuvent être distinguées: l'étiquette communicante; l'identifiant personnel; le traceur; le capteur d'informations.

Étiqueter

L'étiquette communicante est actuellement l'usage le plus prometteur sur le plan économique, notamment dans la logistique et la grande distribution. L'étiquette RFID succède ici au code à barres, avec des performances accrues. L'étiquette identifie chaque produit individuellement , alors que le code à barres n'identifiait que la catégorie. Quand un magasinier passe une palette ou le consommateur un caddie sous un portail de détection, toutes les étiquettes sont scannées en une fraction de seconde et les bases de données sur les produits sont mises à jour. Les étiquettes RFID peuvent

Les dispositifs d'identification à radiofréquences (RFID) sont une pierre d'angle dans la construction des technologies convergentes.

également servir à la sécurisation d'objets (antivol) ou d'animaux domestiques ou d'élevage.

C'est d'abord dans la logistique que les étiquettes RFID ont été mises au banc d'essai, car elles permettent des gains de productivité considérables dans la gestion des flux et des stocks, à condition que les logiciels de gestion des données soient capables de suivre les performances du matériel. Les applications dans la grande distribution n'ont pas encore atteint le seuil de maturité qui permettrait leur diffusion à grande échelle; elles restent limitées à quelques points de vente expérimentaux – bien que Wall-Mart, le leader américain des hypermarchés, utilise intensivement la RFID. Les difficultés de normalisation et d'interopérabilité constituent encore

un frein à la diffusion de l'étiquette communicante. L'acceptabilité de ce changement technologique par les consommateurs ne semble pas problématique tant que les étiquettes RFID n'enregistrent que les produits, sans couplage avec un identifiant personnel.

Identifier

L'identifiant personnel RFID présente en effet un profil plus critique. Dans le cas de l'hypermarché, le couplage entre une carte RFID du consommateur et les étiquettes communicantes peut déboucher sur le profilage, le ciblage des publicités, le contrôle des situations d'endettement. Wall-Mart a ainsi expérimenté un audioguide qui suggère au consommateur les achats à faire en fonction de ses préférences, de son budget et du stock disponible.

Une puce RFID identifiante permet également de stocker des données biométriques, comme des photos ou des empreintes digitales. C'est le cas du passeport biométrique, ou encore de certains systèmes de sécurité qui sélectionnent l'accès individuel à des locaux ou à des équipements.

Lorsque des données personnelles sont incorporées dans une puce RFID communicante, elles relèvent de la législation sur la protection des données et de la vie privée. Les questions de sécurité, de fiabilité et de transparence des identifiants RFID requièrent une évaluation approfondie du point de vue juridique, éthique, politique et social, comme on le verra plus loin dans ce numéro.

Toutefois, de nombreux usages actuels des identifiants RFID sont moins complexes et moins risqués: les cartes de parking, les skipass, l'accès à des installations sportives ou à des bibliothèques, etc.

Suivre à la trace

Une troisième catégorie d'usages concerne le traçage des déplacements, pour autant que les puces émettrices aient une portée suffisante. Les systèmes les plus élémentaires

concernent le suivi des colis ou des bagages, la localisation d'objets ou de véhicules, le télépéage sur autoroute. Des logiciels peuvent assurer une sorte de communication directe entre objets, par exemple entre un colis, sa palette, son camion et sa destination. Par ailleurs, la combinaison de l'identification et du traçage peut permettre d'effectuer des contrôles individualisés, par exemple en suivant à la trace les déplacements et les contacts des employés dans une entreprise.

Capter l'information à la source

Enfin, les dispositifs RFID constituent de puissants capteurs d'information, car ils peuvent être incorporés dans des instruments techniques, des vêtements, des objets domestiques ou des tissus humains. Des logiciels permettent de mettre en réseau des capteurs, des machines et des objets, de les faire interagir, de manière à constituer un "internet des objets". Le cas des implants RFID humains soulève des questions médicales et éthiques qui doivent faire l'objet d'une approche préventive approfondie.

Les défis à relever

À court terme, les principaux défis à relever concernent les normes techniques, la protection de la vie privée, le développement de logiciels capables de gérer de manière fiable et sécurisée les données collectées, la définition d'un cadre juridique et réglementaire approprié, la prise en compte du contexte social et économique de diffusion des innovations.

À moyen terme, face à une technologie qui est à la fois émergente et générique, c'est-à-dire transversale à de nombreux usages, la capacité politique à anticiper les changements et à prévenir les risques est un enjeu essentiel. Un développement débridé de la technologie RFID pourrait s'avérer, à long terme, contre-performant.

La technologie RFID, en quelques mots

Sur le plan technique, les dispositifs RFID se distinguent selon le type d'ondes émises et selon que la puce est active ou passive. Les propriétés techniques influencent le type d'usage qui peut en être fait.

Les puces passives réagissent uniquement au dispositif électromagnétique qui les détecte. C'est le cas de la plupart des étiquettes RFID apposées sur des produits. On peut les assimiler à des codes à barres de deuxième génération. Elles sont aussi utilisées dans le marquage des animaux. Les puces semi-actives sont alimentées en énergie par le dispositif électromagnétique qui les détecte. Elles peuvent être dotées de capteurs, mémoriser les paramètres mesurés et les transmettre en présence d'un dispositif de lecture. Elles sont utilisées à des fins de contrôle à distance ou de diagnostic. Les puces actives sont dotées d'un émetteur récepteur continu et permettent une traçabilité permanente.

Les puces qui émettent dans la gamme des ondes radio ont une faible capacité de mémorisation, mais une longue portée (jusqu'à deux mètres), peu sensible aux obstacles. Les puces de la gamme UHF permettent un meilleur codage, mais leur portée est limitée à moins d'un mètre et les ondes sont facilement absorbées par l'eau ou le métal. Les puces de la gamme des micro-ondes (SHF) sont les plus performantes sur le plan électronique, mais aussi les plus sensibles aux obstacles; leur portée peut s'étendre jusqu'à une dizaine de mètres s'il s'agit de puces actives.

La taille des dispositifs RFID peut varier du centimètre (étiquettes communicantes) au millimètre (implants humains, de la taille d'un grain de riz). Le coût d'une puce RFID est actuellement d'environ 0.25 US$; l'objectif à court terme est de descendre à 0.05 US$, un niveau que les industriels considèrent comme un bon seuil de rentabilité.

La normalisation est un problème non résolu à ce jour. Les plages de fréquences sont différentes en Europe, en Amérique et en Asie. Les normes de codage et d'interopérabilité pour l'échange de données ne sont pas encore universellement établies.

- AWT, *Fiche technique RFID*, Agence wallonne des télécommunications, Namur (www.awt.be).
- European Commission, *Towards a RFID policy for Europe*, Reports from the European consultation on RFID policy, Brussels, 2006.
- Infopôle, *Dossier de documentation de la conférence "Tracking, tracing et objets communicants"*, Namur, novembre 2006 (www.infopole.be).

Environnements intelligents et réseaux ambiants

Enfouir les TIC dans leur environnement, incorporer des éléments d'intelligence dans les objets quotidiens, rendre l'informatique invisible et les réseaux imperceptibles: telles sont les lignes d'action d'une priorité actuelle de la recherche européenne, dénommée *"ambient intelligence"* (intelligence ambiante). D'autres expressions synonymes ont suivi: informatique ubiquitaire, informatique pervasive, systèmes enfouis.

Quand la technologie passe à l'arrière-plan

Selon le programme européen IST (technologies de la société de l'information), le concept d'intelligence ambiante vise à "rendre la technologie invisible, incorporée dans notre entourage quotidien et disponible partout où on en a besoin, comme l'électricité; l'interaction avec la technologie se fait naturellement et sans effort, en utilisant tous nos sens".

Les TIC ubiquitaires constituent un bon exemple de convergence technologique. Elles sont construites à partir de progrès récents dans quatre domaines de la microélectronique: les senseurs, les processeurs, les agents intelligents et la connectivité.

– Les capteurs et senseurs (RFID ou autres) mesurent des paramètres physiques ou biologiques, détectent des modifications de leur environnement, réagissent aux comportements ou aux ordres des utilisateurs.
– La miniaturisation des processeurs permet de concentrer des puissances importantes de calcul et de traitement de données dans des volumes de plus en plus minuscules.
– Les agents intelligents répondent à des signaux en produisant un output qui agit sur leur environnement par des moyens mécaniques, électroniques ou optiques.
– Tous ces dispositifs peuvent être interconnectés de manière invisible, par des réseaux diversifiés (WiFi, Bluetooth, radiofréquences).

Un changement dans les interactions homme machine

Avec ces systèmes ambiants, ubiquitaires, enfouis ou pervasifs, les interfaces avec les utilisateurs deviennent plus interactives. Les objets techniques peuvent réagir à la voix ou au regard, reconnaître des images ou des mouvements, adapter leur action en fonction des informations reçues et traitées. La gamme des applications envisageables concerne la régulation thermique des habitations en fonction de leur occupation, les technologies d'assistance aux personnes handicapées, la surveillance des malades, les soins à domicile, la prévention des risques écologiques, la régulation du trafic. Toutefois, la conception de systèmes qui peuvent s'adapter à des situations imprévues reste encore un défi pour l'ingénierie.

Le degré de maîtrise de l'utilisateur sur ces technologies invisibles est un facteur critique. Les systèmes peuvent réagir à l'insu de l'utilisateur, mais en fonction d'objectifs imposés par lui: ajuster des paramètres de confort domestique, activer une prothèse, émettre une alerte, suggérer une intervention. Il peuvent aussi agir à son insu et sans son assentiment, lorsque les décisions sont enclenchées par des logiciels préalablement paramétrés.

Contrôle, vulnérabilité, pertinence

Les risques associés aux TIC ubiquitaires sont du même type que ceux que l'on connaît déjà avec l'informatique et internet: la protection des données sensibles, la fiabilité des procédures, la vulnérabilité en cas de dysfonctionnement. Toutefois, l'interconnexion généralisée et l'enfouissement dans l'environnement quotidien rendent les risques plus diffus, plus difficiles à percevoir et à contrôler. Certains utilisateurs peuvent se trouver en situation de dépendance par rapport à des environnements intelligents, et d'autant plus vulnérables en cas de problème ou de panne.

> Les environnements intelligents peuvent agir à l'insu de leurs utilisateurs ou sans leur assentiment. La capacité de contrôle est un facteur critique.

La pertinence de solutions technologiques d'avant-garde doit également être évaluée. Dans les grands domaines d'application des environnements intelligents (handicap, santé, transports, régulation énergétique), la technologie n'est qu'un des éléments de réponse, parmi bien d'autres.

- POST, *Pervasive computing*, Parliamentary Office of Science and Technology, POST-note n° 263, London, May 2006.
- European Commission , *Emerging technologies: empowering people in the information society*, Supplement to *CORDIS Focus* n°21, September 2004.
- Commission européenne, *Homme-machine: de nouvelles communications*, dans *RDT Info*, n°51, décembre 2006.

Un besoin d'éthique pour les nanotechnologies

Plusieurs comités d'éthique ont publié des rapports et des recommandations sur les nanotechnologies, leurs perspectives de développement et leurs implications pour la société (voir encadré ci-dessous). Les démarches entreprises en France (CNRS) et au Québec sont semblables, elles abordent ces enjeux d'une manière globale, sous l'angle des technologies convergentes. Quant au Groupe européen d'éthique des sciences et des nouvelles technologies, il s'est focalisé sur le cas des implants TIC chez les êtres humains.

La spécificité des nanotechnologies

Le rapport du CNRS souligne quelques caractéristiques originales du développement des nanotechnologies. Celui-ci est sous-tendu par deux aspirations apparemment contradictoires: la volonté d'explorer le "nanomonde" comme une terre inconnue, sans préjuger des résultats; l'objectif d'utiliser au plus vite les performances des nanotechnologies pour améliorer la capacité de contrôle sur les assemblages atomiques et moléculaires, dans tous les domaines d'application.

Cette tension entre "désir d'émergence" et "désir de contrôle", selon les termes du CNRS, reflète aussi deux approches épistémologiques des nanosciences: une approche systémique et peu déterministe, faisant appel à l'interdisciplinarité; une approche plus cartésienne, fidèle à l'objectif de rendre l'homme "maître et possesseur de la nature".

Dans ce contexte, les discours futuristes sur les potentialités des nanotechnologies méritent l'attention. Certes, ce n'est pas la première fois que des nouveaux domaines de la découverte suscitent des scénarios de fiction, mais le CNRS attire l'attention sur le rôle positif que peuvent jouer ces scénarios dans une réflexion éthique. La fiction a d'abord une fonction heuristique et épistémologique: en situation d'incertitude, les efforts entrepris pour prouver que certains scénarios sont fantasmagoriques éclairent les limites du possible et de l'acceptable. La fiction a aussi une fonction d'intéressement, elle attire l'attention des investisseurs et des responsables des politiques de R&D. Elle a encore une fonction régulatrice et sociale, dans la mesure où elle stimule la prise de conscience des opportunités et des risques, servant ainsi d'amorce à un dialogue entre les chercheurs et le public.

Il faut toutefois éviter le piège d'utiliser le "nano" comme un slogan, à l'instar de cette parodie de définition: "Nano est un minuscule préfixe introduit dans les demandes de fonds afin d'exploiter la générosité inhabituelle du financement de la recherche".

Une exigence de responsabilité et de transparence

Les rapports français et québécois soulignent que les nanotechnologies se développent dans une société déjà sensibilisée aux risques que posent certains choix scientifiques et technologiques. Ils insistent sur la nécessité de tirer les leçons des controverses persistantes à propos des biotechnologies, du nucléaire ou du réchauffement climatique, ainsi que de certaines crises récentes (OGM, vache folle, etc.). L'opinion publique devient plus exigeante par rapport aux experts.

La première exigence concerne la transparence des données et analyses sur les impacts des choix technologiques, notamment en termes de santé, d'environnement et de qualité de la vie. Dans une société qui promeut la démocratie et la participation, le débat sur les risques et les conditions de leur acceptation ne peut pas se dérou-

Quelques avis récents de comités d'éthique

En France, le Comité d'éthique du Centre national de la recherche scientifique (CNRS) a pris en 2004 l'initiative d'étudier les enjeux éthiques des nanosciences et des nanotechnologies, en les plaçant dans un triple contexte: scientifique (la convergence NBIC), politique (globalisation et compétition) et social (un public exigeant et critique à l'égard de l'expertise scientifique). Un avis détaillé et argumenté a été publié en octobre 2006. Il s'adresse en premier lieu aux chercheurs, mais il est rédigé de manière à intéresser le grand public.

Au Québec, la Commission gouvernementale d'éthique de la science et de la technologie a publié en juin 2006 un important rapport intitulé "éthique et nanotechnologies: se donner les moyens d'agir", qui est aussi un excellent document de vulgarisation sur les enjeux sociétaux des nanotechnologies. Des recommandations sont formulées pour les grands domaines d'applications , ainsi que pour des aspects transversaux d'organisation de la recherche et d'encadrement institutionnel et législatif.

Au niveau de la Commission européenne, le Groupe d'éthique de la science et des nouvelles technologies a rendu en mars 2006 un avis sur les aspects éthiques des implants TIC dans le corps humain. Cet avis dresse un inventaire des usages potentiels des implants électroniques humains et formule une série de recommandations sur des mesures de précaution et de protection de la vie privée.

ler uniquement dans des cercles clos d'experts scientifiques. La transparence conditionne la confiance que le public peut accorder à la science et à la technologie.

> Les exigences de responsabilité et de transparence touchent à des représentations et des valeurs face à un domaine technologique naissant, perçu à la fois comme menaçant et fascinant.

La seconde exigence porte sur la responsabilité des chercheurs. Ceux-ci se trouvent face à l'obligation croissante de rendre des comptes et d'exposer clairement non seulement leurs résultats, mais aussi la conscience qu'ils ont des implications pour les citoyens et pour la société en général.

Le débat public est une manière de rencontrer ces exigences. Dans l'actualité toute récente, le cycle d'événements Nanoviv, organisé à Grenoble à l'automne 2006 par divers acteurs du monde scientifique et de la vie associative, illustre bien l'ensemble des problématiques soulevées ici.

Ces exigences de responsabilité et de transparence ne sont pas spécifiques aux nanotechnologies, mais celles-ci touchent à des représentations et des valeurs qui suscitent la sensibilité du public face à un domaine technologique naissant, perçu tantôt comme menaçant, tantôt comme fascinant.

Une réflexion sur les valeurs

Dans son avis sur les implants humains, le Groupe européen d'éthique s'est mis d'accord sur un socle de valeurs qui doivent sous-tendre la formulation de recommandations éthiques. Ces valeurs sont la dignité humaine, l'intégrité et l'autonomie de chaque être humain, la protection de la sphère privée. Sur la base de ces valeurs, quelques principes éthiques sont définis:

– la non-instrumentalisation du corps humain, selon laquelle l'individu ne doit pas être considéré comme un moyen, mais toujours comme une fin en soi;

– le principe de non-ingérence dans la vie privée et de contrôle des individus sur l'usage qui est fait de leurs données personnelles;

– la non-discrimination, l'égalité de traitement, l'accessibilité et la distribution équitables des ressources en matière de santé;

– le consentement libre et éclairé de l'individu pour toute intervention sur son propre corps.

Des conflits de valeurs peuvent se produire, notamment entre la liberté individuelle et les intérêts collectifs; l'élaboration de codes de bonne conduite doit permettre de résoudre ces conflits de valeurs.

Selon le rapport du CNRS, les nanotechnologies se déploient sur un fond de transgression de certaines valeurs fondamentales, notamment la distinction entre nature et artifice, entre l'être humain et les objets techniques. Cette transgression est déjà observable dans les métaphores du langage, quand on parle de machines moléculaires pour décrire aussi bien le fonctionnement d'un artefact que d'une cellule vivante, ou quand on considère les implants humains comme un processus naturel qui s'inscrit dans l'évolution biologique.

Passer des préoccupations aux recommandations

Le rôle de tous les comités d'éthique est de proposer des recommandations; les trois rapports cités dans cet article n'échappent pas à la règle.

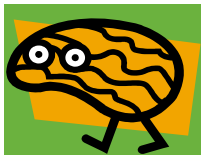
Le CNRS privilégie les recommandations relatives au fonctionnement de la recherche et à son ouverture vers la société: interdisciplinarité, ouverture d'espaces de débat éthique dans les laboratoires, stimulation de la recherche en sciences sociales et humaines en lien étroit avec la recherche technologique, engagement en faveur de la culture scientifique et du débat avec les citoyens.

Le Groupe européen d'éthique propose des recommandations centrées sur le droit, les procédures juridiques et institutionnelles, la déontologie médicale, les codes de bonne pratique pour les chercheurs.

> Dans le domaine des implants humains, le Groupe européen d'éthique s'accorde sur un socle de valeurs: la dignité humaine, l'intégrité et l'autonomie de chaque être humain, la protection de la sphère privée.

Quant au rapport québécois, il s'articule sur les grands domaines d'application des nanotechnologies (santé, environnement, sécurité, performances humaines) et propose, pour chaque thème, des commentaires sur les enjeux éthiques et des recommandations institutionnelles.

- CNRS, *Enjeux éthiques des nanosciences et nanotechnologies,* Comité d'éthique du CNRS, Paris, 12/10/2006.
- Commission d'éthique de la science et de la technologie du Québec, *Ethique et nanotechnologies: se donner les moyens d'agir*, Gouvernement du Québec, juin 2006.
- Groupe européen d'éthique des sciences et des nouvelles technologies, *Ethical aspects of ICT implants in the human body*, Commission européenne, Luxembourg, mars 2005.
- Sur les initiatives de débat public à Grenoble: www.vivagora.org

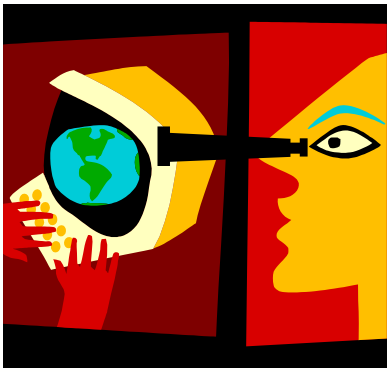


Les risques d'une société sous surveillance

Certaines analyses critiques des technologies convergentes stigmatisent une tendance à organiser la convergence autour d'objectifs de contrôle et de surveillance. La convergence NBIC serait victime d'une sorte de dérive sécuritaire. Divers groupes de pression se sont constitués pour s'opposer à certains projets, notamment dans le domaine de la collecte et de l'utilisation de données biométriques.

Le cas de la biométrie

Ce n'est pas un hasard si de nombreuses inquiétudes se cristallisent sur la biométrie et ses applications en cours de développement: le passeport biométrique, les contrôles d'accès basés sur les empreintes biologiques



numérisées, les implants biométriques, etc. Le principe est simple: chaque individu peut être caractérisé par une série de paramètres biologiques (empreinte digitale, visage, iris, voix, échantillons d'ADN), qui forment une combinaison unique et qui peuvent aujourd'hui être numérisés. L'enjeu éthique est tout aussi évident: les caractéristiques biométriques font partie du corps d'un individu, dans quelle mesure peut-on les stocker, les communiquer, les vérifier à l'insu ou sans l'assentiment de la personne concernée ?

À la demande du Parlement européen, l'Institut de prospective technologique (IPTS) a évalué les différents impacts du développement de la biométrie, dans le cadre des technologies convergentes. Cette étude repose sur deux postulats. D'une part, la diffusion des applications biométriques dépend de leur acceptabilité sociale, qui sera facilitée par leur usage dans les passeports et autres systèmes d'identification; les applications commerciales suivront, à condition que les cadres législatifs s'adaptent. C'est pourquoi l'IPTS recommande que les objectifs précis de chaque application biométrique soient clairement définis, de façon à favoriser la confiance des citoyens. D'autre part, il faut reconnaître les limites de ces technologies: leur fiabilité n'est pas absolue, elles sont vulnérables, elles ne resteront pas inviolables. Des procédures alternatives doivent toujours être prévues en cas de panne ou de dysfonctionnement des systèmes.

La société de la surveillance

Aux yeux des opposants à la biométrie, il est peu probable que ces conclusions éloignent le spectre d'une société de la surveillance. Selon un rapport rédigé pour la conférence européenne des commissaires nationaux à la protection des données, cette société de la surveillance existe déjà et elle repose largement sur la technologie: bases de données, RFID, biométrie, traçage, tri social, marketing ciblé, etc.

Les législations de protection des citoyens sont souvent réactives, elles suivent la technologie mais ne l'anticipent pas, si bien que les nouveautés se développent toujours dans un contexte peu encadré. Les progrès technologiques requièrent une nouvelle approche du concept de vie privée, qui devrait être basé sur une évaluation continue des facteurs constitutifs de la vie privée et de leur évolution.

Les commissaires nationaux soulignent que les systèmes de surveillance invisibles, incontrôlés, incompréhensibles ou excessifs peuvent créer de l'insécurité au lieu de la sécurité. Ils peuvent aussi générer la marginalisation ou l'exclusion. La réglementation de la protection de la vie privée est insuffisante. C'est l'ensemble des dispositifs qui créent et entretiennent la confiance qui doivent être pris en considération pour que surveillance, liberté et démocratie restent compatibles.

- IPTS, *Biometrics at the frontiers: assessing the impact on society*, EUR21585-EN, JRC Institute for prospective technological studies, Sevilla, February 2005.
- Murkami Wood D., Ball K., *Un rapport sur la société de surveillance*, Rapport du *Surveillance Studies Network* pour la 28ème conférence européenne des commissaires à la protection des données et à la vie privée, Londres, novembre 2006.
- Des points d'entrée vers des groupes de pression "anti-puces": www.jameh.org; www.stoppuce.be; www.ines.sgdg.org

FTU
Centre de recherche Travail & Technologies
ASBL Association pour une
Fondation Travail-Université
Rue de l'Arsenal 5, B-5000 Namur
Tél. 081-725122 - fax : 081-725128
E-mail: pvendramin@ftu-namur.org
http://www.ftu-namur.org

Conception, rédaction et mise en pages:
Patricia Vendramin et Gérard Valenduc

Le Lettre EMERIT est publiée avec le soutien financier du Fonds National de la Recherche Scientifique (FNRS)

FNRS

Editeur responsable: G. Valenduc

Imprimé par Denef SPRL, Louvain-la-Neuve