Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitudes

Ayse CEYHAN

Ayse Ceyhan est docteur en science politique et enseignante à l'IEP de Paris. Ses dernières publications sont : « La biométrie, une technologie pour gérer les incertitudes de la modernité contemporaine », Cahiers de l'INHES*, printemps 2005, n°56 ; « Identité et identification au prisme de la technologie », www.ihej.org/ressources/ceyhan_20_03_06.*

Quels sont les liens entre technologie et sécurité et comment étudier la technologisation fulgurante de la sécurité ? Quels sont les enjeux et les processus qui mènent les pouvoirs publics à célébrer les nouvelles « technologies de sécurité », telles que les techniques de surveillance et d'identification, comme l'instrument le plus puissant de lutte contre les risques et les menaces ? Quelles sont, enfin, les logiques de diffusion à l'œuvre faisant des « technologies de sécurité » un dispositif presque banal de la vie quotidienne ? Pour examiner ces questions, nous nous proposons dans cet article – et plus généralement dans ce numéro – de dépasser les approches déterministes et essentialistes des rapports technologie / sécurité et d'adopter une analyse touchant aux contextes et dynamiques.

Une analyse des technologies ne saurait se passer d'un examen des termes « technique » et « technologie », souvent confondus dans le langage courant. Toutefois, leur distinction semble difficile en raison « *de la rhétorique et des usages sociaux* [1] ». En remontant aux origines grecques, on dira que la « technique » – qui vient de la *technê* – se comprend à la fois comme art (artefact) et comme métier. La « technologie », terme employé pour la première fois au XVII[e] siècle, se rapporte quant à elle à la convergence entre *technê* et sciences et signifie « traité »

1 . Sfez L., *Technique et idéologie. Un enjeu de pouvoir*, Paris, Seuil, 2002, p. 285. Sur les usages rhétoriques, Sfez écrit dans cet ouvrage : « *Il est noble de parler de la "technologie" quand on est politique ou haut fonctionnaire, ces élites réservant le terme "technique" à des affaires d'artisanat et de plomberie* ».

ou « science des règles d'un art ». Mais distinguer clairement ces deux termes paraît ardu et c'est ainsi que des sociologues comme Lucien Sfez ou des philosophes comme Michel Serres ont fini par abandonner l'idée de les séparer conceptuellement [2]. Compte tenu de cette difficulté et de l'usage généralisé du terme technologie, nous dirons que celui-ci relève à la fois de la *technê* et des savoirs, non seulement d'un point de vue scientifique, mais aussi d'un point de vue philosophique et pratique. Dans cette optique, la technologie se rapporte à une réflexion sur les techniques, leurs rapports avec les sciences fondamentales, les conséquences politiques, sociales, symboliques et éthiques de leur développement ainsi que leur impact sur les relations humaines et leur environnement [3]. Quant à son usage dans le monde industriel, la technologie renvoie à un ensemble de matériaux, de procédés et d'outillages destiné à une production industrielle.

A partir de ces éléments, nous proposons d'établir un lien avec le concept de dispositif développé par Michel Foucault [4]. Bien que, de nos jours, l'usage de ce terme soit devenu polysémique [5], il pourrait être replacé dans son cadre technico-scientifique au sens d'une formation mixte de technique et de symbolique, c'est-à-dire de support d'imaginaire. Dans une acceptation purement technique, le dispositif est entendu comme un « *ensemble de pièces constituant un appareil, une machine* [6] ». Dans un sens plus large, il englobe « *tout agencement d'éléments humains ou matériels, réalisé en fonction d'un but à atteindre* [7] ». En se référant aux travaux de Michel Foucault et de Gilles Deleuze, on peut dire que le dispositif est un ensemble constitué par des relations entre divers éléments hétérogènes mais néanmoins connectés, comme la machine (la technique), les procédés, les énoncés, les réglementations, l'environnement et les moyens symboliques et relationnels qui modélisent les comportements individuels et sociaux [8]. Cette défini-

2 . Pour Sfez, une des raisons de cette difficulté relève du manque de cohérence entre les philosophes qui fondent leurs définitions sur des présupposés différents qui sont soit essentialistes (Heidegger, Jangada), soit épistémologiques (Granger) ou épistémologico-systémique, sociologique et historique (Moscovici), etc. Sfez L., *ibid*., p. 291. Michel Serres déplore aussi cette perte de distinction. Pour lui, « *le terme technologie désignait, naguère en langue française, l'étude raisonnée des outils et des machines, dans un traité discursif sur les arts et les métiers. Sous l'influence des usages de la langue anglaise* […]*, il semble usité de plus en plus à la place du mot : technique et dans le même sens que lui* ». Voir : Serres M., *Atlas*, Paris, Champ Flammarion, 1994, p. 191.

3 . Nous empruntons cette définition à Morfaux L.-M., *Vocabulaire de la philosophie et des sciences humaines*, Paris, Armand Colin, 1980, p. 359.

4 . Foucault M., *Surveiller et punir. La naissance de la prison*, Paris, Gallimard, 1975 ; *Histoire de la sexualité* t. I, « La Volonté de savoir », Paris, Gallimard, 1976. Pour une analyse de la conception foucaldienne du dispositif voir : Deleuze G., « Qu'est-ce qu'un dispositif ? » in *Michel Foucault philosophe. Rencontre internationale*, Paris 9, 10, 11 janvier 1988, Paris, Seuil, 1989, pp. 185-195.

5 . Il est déployé pratiquement dans tous les champs de savoir et de pratique. Ainsi, on parle de dispositif communicationnel, de dispositif administratif, de dispositif policier, de dispositif psychiatrique, etc.

6 . *Le Petit Larousse*.

7 . « Le dispositif entre usage et concept », *Hermès*, CNRS, n° 25, 1999, Introduction.

8 . Pour cette description nous nous sommes inspirés de Deleuze G., *op. cit*. Voir également la définition fournie par Peraya D., « Médiation et médiatisation : le campus virtuel », *Hermès*, CNRS, n° 25, 1999, pp. 153-167.

tion qui situe la connexion entre la *technê*, son environnement et l'homme peut permettre d'analyser les technologies de sécurité qui, par leur introduction rapide dans la vie quotidienne des individus, participent à la modélisation de leurs comportements et attitudes.

Toutefois, à la lumière des travaux de Gary T. Marx [9], de Zygmunt Bauman [10] et d'Andrew Feenberg [11] entre autres, nous pouvons affirmer que la technologie ne se réduit pas seulement à un dispositif technique, scientifique et symbolique, mais qu'elle est également conditionnée par le contexte dont elle est le produit. Nous examinerons donc l'adoption des technologies d'identification, de surveillance et de traçabilité dans le contexte d'incertitudes et d'inquiétudes généré par la « *modernité liquide* » (Bauman), la « *société mondiale du risque* » (Beck) et les transformations de la violence dont le point culminant a été atteint par les attentats du 11 septembre 2001. Cependant, contrairement à une idée largement répandue, le terrorisme ne constitue pas l'événement déclenchant la technologisation de la sécurité. Comme nous le verrons plus loin, l'introduction de la haute technologie dans le champ de la sécurité a commencé bien auparavant, dès les années 1980, avec la lutte contre la drogue et l'immigration clandestine [12]. Les attentats du 11 septembre n'ont fait que renforcer la globalisation de ce processus. Par ailleurs, bien que, comme l'a noté Ulrich Beck, ces attentats aient débouché sur une « *construction transnationale des Etats citadelles fondés sur la surveillance* [13] », l'Etat n'est pas le seul acteur impliqué dans le processus de la technologisation de la sécurité. De façon volontaire et parfois forcée – comme on peut le voir dans le cadre de la lutte antiterroriste-, il compose avec d'autres acteurs comme les entreprises et les organismes internationaux par un jeu de délégation, de coopération, de transaction, d'échange et de contrat. Tout porte à penser qu'à l'heure de la globalisation, son action et sa légitimité dépendent de la relation de coopération et d'échange – qu'on appellera « gouvernance » – qu'il établit avec des acteurs privés, transnationaux et internationaux impliqués dans la production et l'adoption des nouvelles technologies de sécurité [14].

---

9 . Marx G.T., « Technology and social control », in Smelser N., Baltes P. (eds.), *International Encyclopedia of the Social and Behavioral Sciences*, Oxford, Pergamon, 2002, p. 15506-15511 ; *Undercover Police Surveillance in America*, Berkeley, University of California, 1990 ; « La société de sécurité maximale », *Déviance et Société*, 12 (2), 1998, pp. 33-52 ; « An ethics for the new surveillance », *The Information Society*, vol.14, n° 3, 1998 ; « Technologies de sécurité et société », *Les Cahiers de la sécurité intérieure*, 3/1995, pp. 9-15.

10 . Bauman Z., *Liquid Modernity*, London, Polity Press, 2000 ; *Globalization, The Human Consequence*, London, Polity Press, 1998 ; *Liquid Love*, London, Polity Press, 2004.

11 . Feenberg A., *(Re)penser la technique. Vers une technologie démocratique*, Paris, La Découverte / Mauss, 1999.

12 . Voir Ceyhan A., « Sécurité, frontières et surveillance aux Etats-Unis après le 11 septembre », *Cultures & Conflits*, n° 53, 2004, pp. 113-145.

13 . Beck U., *Pouvoir et contre-pouvoir à l'heure de la mondialisation*, Paris, Alio/Aubier, 2003, p. 182 et p. 186.

14 . Pour une analyse plus poussée de la gouvernance à l'heure de la mondialisation voir Laidi Z., *Adieu Bodin, Souveraineté et mondialisation*, Institut universitaire d'études du développement (INED), Genève, mai 2003.

La gouvernance libérale

Le terme « gouvernance [15] » est généralement employé pour désigner des situations où le rôle de l'Etat s'affaiblit au profit d'organisations internationales, d'entreprises, d'ONG, d'associations, etc. Dans notre approche, la gouvernance revêt deux significations complémentaires. La première est la constitution d'un réseau complexe d'acteurs comprenant les Etats, les agences publiques, privées et transnationales de sécurité, les entreprises, les organisations internationales comme l'Organisation de l'Aviation civile internationale (OACI) [16], l'Union européenne, les experts, les juristes, les compagnies d'aviation et les associations de défense des droits fondamentaux, qui participent à la production, à la diffusion, à l'adoption, à l'évaluation et à la critique des technologies de sécurité. La constitution de ce réseau hétéroclite n'est toutefois pas neutre. Elle engage des relations de pouvoir et d'intérêt tissant entre les acteurs des alliances plus ou moins durables. Le succès ou l'échec de l'innovation technologique dépend d'ailleurs de la négociation entre les différents acteurs qui composent ce réseau [17].

La seconde signification est dérivée de la notion de « gouvernementalité » développée par Michel Foucault [18]. Dans son analyse des « *arts de gouverner* », allant du pouvoir pastoral à la rationalité libérale en passant par la raison d'Etat, Foucault a montré que le pouvoir ne se réduit pas au seul contrôle du territoire et de l'institution, mais s'étend au gouvernement des hommes, des individus ou des collectivités [19]. Il a appelé « gouvernementalité » le régime de pouvoir mis en place au XVIII[e] siècle qui « *a pour cible principale la*

15 . Pour la notion de gouvernance voir Barrot L., « Gouvernance », *Cités*, 2002 ; Leca J., « Gouvernance et institutions politiques. L'Etat entre sociétés nationales et globalisation », in Foucault J.B., Fraisse R. (dir.), *La France en perspective*, Paris, Odile Jacob 1996 ; « Commission on global governance », *Our Global Neighborhood*, Oxford, Oxford University Press, 1995.

16 . L'Organisation de l'Aviation civile internationale est une institution spécialisée de l'ONU. Créée en 1947, elle a pour but de faciliter les vols internationaux et d'en augmenter la sécurité. Elle établit les règles et normes techniques qui permettent d'uniformiser les règlements de fonctionnement des services aériens et de voyage des passagers. C'est elle qui fixe les normes techniques des passeports.

17 . Voir Callon M., *La Science et ses réseaux,* Paris, La Découverte, 1989 ; « Some elements in a sociology of translation: domestication of scallops and fishermen of the St Brieuc Bay », in Low J. (ed) *Law, Power, Action, Belief*, Routledge, London, 1986.

18 . Le concept de gouvernementalité a inspiré un grand nombre de travaux français et anglo-américains en relations internationales, sciences politiques et philosophie. Voir Bigo D., « Les nouvelles formes de la gouvernementalité : surveiller et contrôler à distance », in Grangeon M.-C., *Repenser avec Foucault. Théorie critique et pratique politique*, Paris, Karthala, 2005 ; Sennelard M., « Michel Foucault, gouvernementalité et raison d'Etat », *Pensée politique*, n°1, 1993, pp. 276-303 ; Moss J., *The Later Foucault. Politics and Philosophy*, London, Thousands Oaks et New Delhi, Sage Publications, 1998.

19 . Foucault dira dans la leçon du 8 février 1978 : « [...] *c'est qu'on n'y gouverne jamais un territoire, on n'y gouverne jamais une structure politique. C'est qu'on gouverne, c'est de toutes façons des gens, ce sont des hommes, ce sont des individus ou des collectivités* ». Foucault M., *Sécurité, territoire, population*, Cours au Collège de France, 1977-1978, Paris, Gallimard/Seuil, 2004, p. 126.

population, pour forme majeure de savoir l'économie politique, pour instrument technique essentiel les dispositifs de sécurité [20] ». Portant au départ sur les techniques de gouvernement qui sous-tendent la formation de l'Etat moderne [21], la gouvernementalité a ensuite été entendue « *au sens large de techniques et procédures destinées à diriger la conduite des hommes. Gouvernement des enfants, gouvernement des âmes ou des consciences, gouvernement d'une maison, d'un Etat ou de soi-même* [22] ». Dans cette acceptation, la gouvernementalité ne permet pas seulement d'appréhender les techniques et les procédures par le biais desquelles s'exerce le pouvoir de l'Etat, mais sert plus généralement de grille d'analyse pour toutes les relations de pouvoir en général, et celles qui gouvernent la vie et le vivant en particulier [23].

Dans le contexte de la globalisation, ces techniques et procédures ont donné lieu à un nouvel art de gouvernement des hommes et des choses, que Julian Reid et Michael Dillon ont nommé « *gouvernance libérale globale* [24] ». Reposant sur des principes (néo)libéraux déjà anciens mais reformulés avec la globalisation, la gouvernance libérale correspond à un régime complexe de pouvoir qui porte sur la gestion du vivant. Elle s'exerce par la globalisation d'un certain nombre de techniques sophistiquées dont l'objet est de procéder à un examen minutieux des caractéristiques intimes des populations afin de remodeler leur comportement en fonction des besoins de la société libérale [25]. Les nouvelles technologies de sécurité, comme la biométrie et les systèmes de surveillance dits « intelligents », représentent bien ces techniques. Prenant l'individu comme objet focal, leur objectif est de gouverner la sphère d'activité que Jürgen Habermas avait nommée « *le monde vécu* » (« *Lebenswelt* [26] »). Pour ce faire, elles commencent par ramener l'identité (au sens d'*ipse* [27]) et les mouve-

20 . Foucault M., *Sécurité, territoire, population*, *op. cit*., p. 111. Nous empruntons cette note à Sennelart M., « Situation des cours », in *Sécurité, territoire, population, op. cit*., p. 406.

21 . Dans ce sens, la gouvernementalité est définie comme « *la manière dont la conduite d'un ensemble d'individus s'est trouvée impliquée de façon de plus en plus marquée, dans l'exercice du pouvoir souverain* », in *Résumé des cours 1970-1982*, Paris, Julliard, 1989, p. 101.

22 . Foucault M., *Dits et Ecrits, 1954-1988*, Paris, Gallimard, 1994, p. 124 ; Résumé du cours « Du gouvernement des vivants », *op. cit.*, p. 123.

23 . Sennelart M., *op. cit*., p. 407.

24 . Dillon M., Reid J., « Global liberal governance: biopolitics, security and war », *Millennium: Journal of International Studies*, vol. 30, n° 1, pp. 41-66.

25 . *Ibid*., p. 41.

26 . Le monde vécu (*Lebenwelt*) est un concept développé par Habermas pour signifier le monde où se déploie l'action des membres de la société. Il s'agit de rendre compte de cette action du point de vue de celui qui agit. Dans le monde vécu, les actions sont coordonnées par les orientations et communications intersubjectives. Elles engagent le domaine subjectif, le domaine intersubjectif et le domaine des normes et valeurs cognitives et instrumentales. En somme, il s'agit du domaine de la vie privée. Voir *Théorie de l'agir communicationnel,* t. 1 « Rationalité de l'agir et rationalité de la société », Paris, Fayard, 1987 et *Droit et démocratie. Entre faits et normes*, Paris, Gallimard, coll. « Essais », 1997.

27 . Pour une analyse plus poussée de cette notion d'« identité *ipse* », se référer à Ricoeur P., *Soi-même comme un autre*, Paris, Le Seuil, 1991 ; voir Ceyhan A., « Enjeux d'identification et de surveillance à l'heure de la biométrie » dans ce numéro et Garapon A., *Audition par la CNIL*, le 14 avril 2005.

ments d'un individu de l'anonyme au connu en les catégorisant et les transformant en données informatiques.

Toutefois, cette gouvernance qui permet la participation d'un nombre croissant d'acteurs étatiques et extra-étatiques à la gestion du vivant et de l'(in)sécurité est génératrice de problèmes éthiques, sociaux et déontologiques dont l'impact sur le monde vécu s'accroît de jour en jour, au fil de l'intrusion des nouvelles technologies d'identification et de surveillance dans la vie quotidienne.

L'obsession technologique

Depuis la fin de la bipolarité, on assiste à un développement considérable du marché des technologies de sécurité qui s'est intensifié avec les attentats de New York et de Washington ainsi que ceux de Madrid du 11 mars 2004 et de Londres du 7 juillet 2005. Désormais, il ne se passe pas un jour sans qu'on entende des appels en faveur de l'adoption des technologies de sécurité comme le détecteur à rayons X, la vidéosurveillance dite « intelligente », le passeport à identifiants biométriques, le permis de séjour biométrique, les badges biométriques, les cartes à puce, etc. Sous la pression des Etats-Unis, suivis de près par la Commission européenne et le G8, les pouvoirs publics se précipitent pour adopter ces technologies à une vitesse grandissante. Ces technologies sont perçues comme les instruments les plus « scientifiques » de prévention et d'anticipation des menaces par leur mode d'identification des individus à partir de ce qui constitue leur unicité, leur création de profils de comportements à risque et leur interconnexion avec des bases de données [28].

Toutefois, la question cruciale consiste à savoir si la technologie peut ou non tout prévoir. En effet, est-il possible de tout anticiper ? Que faire en cas d'événement imprévu ? D'autre part, la technologie peut-elle permettre de vaincre les peurs et les angoisses incertaines qu'Elias avait décrites [29] ? De nombreux auteurs comme Gary T. Marx [30], Frédéric Ocqueteau [31] et François Guéry [32] ont émis

28 . On peut citer comme exemple le système informatisé CAPSS (*Computer Assisted Passenger Screening System*) auquel a succédé CAPSS2, destiné à permettre le profilage des passagers à risque et leur dépistage avant l'entrée aux Etats-Unis. A l'aide de l'analyse des données PNR détenues par les compagnies d'aviation, il attribue à chaque passager au moment du check in un code de couleur correspondant à son niveau estimé de dangerosité.

29 . Elias N., *La Civilisation des mœurs* (1939), Paris, Agora Press Pocket, 1990. Elias parlait notamment d'« *une forme spécifique d'angoisses intérieures à demi conscientes naissant de la peur de la rupture des barrières que la société impose à l'homme civilisé* », p. 245.

30 . Marx G.T., *op. cit*.

31 . Ocqueteau F., « Technologies de sécurité et modalités publiques et privées de l'ordre : l'exemple français », in Shapland J., Van Outrive L. (dir), *Police et Sécurité. Contrôle social et interaction public/privé*, Paris, L'Harmattan, 2000, pp. 127-137 ; *Polices entre Etat et marché*, Paris, Presses de Sciences Po, 2004.

32 . Guery F., « La sécurité comme politique et comme idéologie », in Dourlens C., Gailland J.-P., Theys J., Vidal-Naquet P.-A. (dir), *Conquête de la sécurité, gestion des risques*, Paris, L'Harmattan, 1991, pp. 253-256.

des doutes quant à la toute puissance de la technologie et ses capacités de prévoir et de gérer les risques et les dangers. Ils ont analysé les raisons de la production de cette croyance au travers des enjeux de pouvoir bureaucratiques, économiques et symboliques. Examinant le rôle des experts, Frédéric Ocqueteau a montré que les ressorts de cette croyance étaient ambivalents et fragiles dans un environnement reposant sur le manque d'information et le peu d'expérience que les individus possèdent du bon fonctionnement de ces technologies [33]. Cependant, malgré ce constat, les technologies de sécurité continuent de croître à une vitesse fulgurante. A chaque attentat terroriste commis ou dès qu'un risque d'attentat devient plus prégnant, les systèmes de détection les plus sophistiqués sont immédiatement écoulés sur le marché. Comment expliquer cet engouement pour la technologie ? Est-ce le résultat de l'effet performatif des discours sur la toute puissance de la technologie ou d'autres dynamiques sont-elles en jeu ?

Dépasser les déterminismes et les essentialismes

Sur le plan analytique comment étudier la technologisation de la sécurité ? Cette question étant posée une autre vient aussitôt à l'esprit, celle de savoir si c'est la technologie qui détermine ce phénomène par son efficacité, sa flexibilité et l'appel de son marché, ou bien si c'est le besoin de sécurité qui incite les gouvernements et les particuliers à opter pour davantage de technologie. Au niveau des acteurs, cela revient à se demander si ce sont les entreprises, les experts ou les hommes politiques qui génèrent cet engouement. Toutefois, nous pensons que cette façon de poser la question est circonstancielle et ne nous permet pas en soi de comprendre les véritables enjeux liés au contexte actuel et aux logiques à l'œuvre dans le développement de ce phénomène. Elle risque en effet de nous conduire à ne prendre en considération qu'un groupe d'acteurs particuliers, de le représenter par une image monolithique ne laissant pas entrevoir les conflits qui peuvent exister au sein de ce groupe et de concevoir la technologisation de la sécurité comme le simple résultat de la défense de ses intérêts particuliers.

De même, nous pensons que les analyses en terme d'efficacité ne permettent pas de saisir la spécificité sociale et historique des technologies. Aux yeux de ceux qui pratiquent la technologie, les nouvelles technologies de sécurité doivent être appréhendées en fonction de leur efficacité. Toutefois, celle-ci ne peut pas être mesurée avec justesse en raison du manque de recul face aux technologies émergentes, comme la biométrie, en constante évolution. Il faut donc dépasser cette obsession de l'efficacité et adopter une posture analytique qui ne conçoit pas la technologie comme phénomène autonome mais comme le produit d'un contexte particulier, qui examine les effets sociaux, politiques et éthiques qu'elle induit.

33 . Ocqueteau F., *Polices entre…*, *op. cit*., p. 12.

Ainsi, sur le plan analytique, nous ne souhaitons pas nous limiter aux visions déterministes et essentialistes développées en particulier en philosophie en matière de technique. Ces deux visions appréhendent la technologie comme un phénomène décontextualisé et transhistorique [34]. Selon les thèses déterministes, dont les origines remontent au discours de la modernité, la « technique » est la représentation par excellence du progrès [35]. Elle n'est pas seulement un instrument de la modernité, mais le moteur même du système social. En conséquence, toutes les institutions sociales et politiques doivent s'adapter à ses impératifs. D'où la thèse de l'universalité technologique qui implique le primat de l'expertise scientifique sur le politique, sur le droit et la volonté des individus, non seulement au niveau national, mais aussi sur le plan planétaire. Comme nous le savons, cette vision a été fortement contestée par Foucault [36] et Marcuse [37] qui, en fonction de leurs présupposés analytiques et politiques respectifs, ont condamné l'idée faisant de la rationalité instrumentale la seule voie pour atteindre le progrès.

L'essentialisme, dont les représentants les plus connus sont Martin Heidegger [38] et Jacques Ellul [39], considère que la technique réduit tout à des fonctions et à des matières premières [40]. Il établit une distinction ontologique entre la technique et le sens, privilégiant la rationalité et l'efficacité de la première et refusant de prendre en considération le second. Dans cette approche, la technique est présentée comme autonome et possède sa propre logique. Elle est en conséquence détachée de l'expérience. Heidegger a formulé cette position en termes ontologiques. Pour lui, la technique est une étape dans l'histoire de l'Etre, c'est un mode de « dévoilement » de notre temps, non pas par son utilité parce qu'elle permet aux choses d'apparaître telles qu'elles sont au plus profond d'elles-mêmes, sans faire allusion à la volonté et à l'action préalables des hommes. Dans ce sens elle n'est pas un instrument, elle forme une culture du contrôle universel [41]. Et ce faisant, elle absorbe ses créateurs en les incorporant dans le mécanisme de transformation de tout ce qu'elle touche en matières premières et menace leur survie spirituelle ainsi que matérielle [42]. Or,

34 . Pour une présentation approfondie de ces thèses voir Feenberg A., *(Re)penser la technique*, *op. cit*., pp. 23-74.
35 . Voir les thèses de Marx, Darwin, Saint-Simon.
36 . Foucault M., *Surveiller et punir*, *op. cit*.
37 . Marcuse H., *One Dimensional Man*, Boston, Beacon Press, 1964.
38 . Pour Heidegger, le développement technique n'est pas à proprement parler un phénomène social et humain, il procède bien plutôt d'un envoi de l'Etre. Ce qui conduit à une dénégation de l'action politique ainsi que de toute possibilité pour l'homme de pouvoir contrôler la technique. Voir Heidegger M., *The Question Concerning Technology*, New York, Harper, 1977 (« La question technique », in *Essais et conférences*, Paris, Gallimard, 2003).
39 . Pour Jacques Ellul, le phénomène technique est caractérisé par son autonomie. Voir Ellul J., *The Technological Society*, New York, Vintage, 1964 (*Le Système technicien*, Paris, Calmann-Lévy, 1977).
40 . Feenberg A., *op. cit*., pp. 23-25.
41 . *Ibid*, p.25.
42 . Voir Heidegger M., « La question technique » , *Essais et conférences, op. cit.*

comme le remarque Andrew Feenberg, la technique doit inclure la dimension de l'expérience et du sens, « *puisque l'expérience que les gens ont des dispositifs a une influence sur l'évolution de leur conception* [43] ». Pour cet auteur, ce que l'essentialisme conçoit comme une distinction ontologique entre la technique et le sens est plutôt un terrain de lutte entre différents acteurs – dont les usagers – qui entretiennent des relations différentes avec la technique et le sens [44]. Qu'il s'agisse de contestations scientifiques et politiques, de critiques des juristes et des philosophes ou bien de l'intervention du public en faveur ou contre une technologie, les luttes sont au cœur de l'avènement de changements profonds comme l'attestent le cas de la médecine ou de l'informatique [45].

Plutôt que de considérer la technologie comme autonome et de la réduire à la recherche de l'efficacité, nous pensons qu'elle joue de multiples rôles dans la vie de l'individu. Elle forme un mode de vie et une culture, induit des contraintes et modèle des comportements et attitudes, y compris des attitudes de résistance.

Les contextes et dynamiques

Si l'usage des technologies de sécurité s'est très largement accru à partir des attentats du 11 septembre sous l'impulsion des Etats-Unis, cette évolution était déjà présente bien antérieurement. Dès la moitié des années 1970, pour contrôler la frontière avec le Mexique, la *Border Patrol* [46] américaine avait adopté les technologies de surveillance et d'identification conçues pour les militaires pendant la guerre du Vietnam [47]. En Angleterre, dans les années 1980, la vidéosurveillance avait été adoptée comme dispositif de lutte contre le crime et le terrorisme – en particulier contre les activités de l'IRA – Elle a été ensuite étendue à la lutte contre le hooliganisme [48]. Rappelons également que l'Angleterre est le pays qui, avec le Pays de Galles, possède de loin la plus grande collection de profils ADN : la *National DNA Database*, devenue opérationnelle dès 1995. L'Allemagne a, quant à elle, déployé des technologies de surveillance et de traçabilité connectées aux bases de données dès les années 1980 dans le cadre de la lutte contre la Faction de l'Armée rouge. En France, le recours aux nouvelles technologies a commencé vers la fin des années 1970, avec le projet d'informatiser la carte nationale d'identité pour rendre le document plus fiable face à l'usurpation et le vol [49]. Cette initiative s'est d'abord

43 . *Ibid*., p. 17.
44 . *Ibid*.
45 . *Ibid*., p. 13.
46 . La police des frontières.
47 . Voir Ceyhan A., « Sécurité, frontière et surveillance aux Etats-Unis après le 11 septembre », *op. cit*.
48 . Voir l'article de Laurent Laniel et de Pierre Piazza dans ce numéro : « Une carte nationale d'identité pour les Britanniques : l'antiterrorisme au cœur des discours de justification ».
49 . Voir Piazza P., *Histoire de la carte nationale d'identité*, Paris, Odile Jacob, 2004, pp. 305-340.

heurtée à une forte hostilité en raison de la tradition française de protection de la vie privée qui a abouti à la loi Informatique et liberté du 6 janvier 1978. Elle s'est néanmoins soldée par l'adoption d'une carte dite « sécurisée ». L'informatisation des documents d'identité a été ensuite étendue aux cartes de séjour des étrangers. Dans les années 1990, les techniques d'identification comme la biométrie d'empreintes digitales ont été introduites pour les demandeurs d'asile et les étrangers en situation irrégulière, avant de s'étendre à tous les étrangers vivant sur le sol français. Quant aux technologies de surveillance, c'est en 1995 avec la loi de Programmation relative à la sécurité qu'un cadre juridique a été adopté pour la vidéosurveillance.

Au niveau européen, les technologies de surveillance ont été adoptées dans le cadre de la sécurisation de la frontière germano-polonaise avant l'entrée de la Pologne dans l'Union. Les technologies d'identification biométriques ont, elles, été introduites dans le cadre de l'européanisation des politiques des visas dès le plan d'action de Vienne adopté par le Conseil des ministres JAI (Justice et Affaires intérieures) le 3 décembre 1998, confirmé ensuite lors du Sommet de Tampere des 15 et 16 octobre 1999 [50]. La décision d'intégrer les éléments biométriques a été prise dans le cadre de la mise en place d'une base de données destinée à établir l'identité des demandeurs d'asile et des personnes appréhendées lors du franchissement irrégulier d'une frontière extérieure à la communauté (Eurodac) [51].

Toutefois, depuis leur adoption, ces systèmes ont suscité de nombreuses critiques portant sur leur inefficacité (la vidéosurveillance), leurs failles de sécurité (les systèmes de communication) ainsi que leur propension à porter atteinte aux droits fondamentaux (notamment par le déploiement des bases de données). Malgré ces critiques, les attentats terroristes – dont ceux de Londres – ont été l'occasion pour les Etats de prendre la décision politique de recourir aux technologies de sécurité, balayant du même coup les objections formulées en termes de sécurité des systèmes, de coût et de protection des droits fondamentaux.

Le contexte dans lequel les technologies de sécurité ont été adoptées est caractérisé par la conjugaison de plusieurs dynamiques : l'accélération de la « *modernité liquide* », l'émergence de nouveaux risques et incertitudes, la privatisation de la sécurité, la mise en place d'un système global de surveillance et la diffusion du paradigme technologique dans la vie de tous les jours.

---

50 . Voir « De Tempere à Séville : bilan de la sécurité européenne », *Cultures & Conflits*, n°45-46, printemps-été 2002.

51 . Voir l'article de Sylvia Preuss-Laussinotte « L'Union Européenne et les technologies de sécurité » dans ce numéro.

L'accélération de la « modernité liquide »

L'expression métaphorique « *modernité liquide* » a été développée par Zygmunt Bauman pour caractériser la forme contemporaine de la modernité, qui est passée d'un « *état solide* » à un « *état liquide* » avec les évolutions de la globalisation et de la transnationalisation [52]. Contrairement à la « *modernité solide* », que l'on peut symboliser par la technologie lourde et fixe comme dispositif et le Panoptique comme système de surveillance, « *la modernité liquide* » se caractérise par les technologies nouvelles, à l'instar des puces et des microprocesseurs, et par un système de surveillance que l'on peut caractériser de « post-panoptique [53] ». Ses principaux traits sont la fluidité, la mobilité et l'interconnectivité entraînant une déterritorialisation des rapports de pouvoir, une privatisation de l'espace public, un déclin des institutions politiques traditionnels comme les partis politiques et les syndicats, et une déstructuration des institutions sociales générant la dilution des notions fondamentales de vivre ensemble comme la solidarité, l'amitié, le voisinage, etc. Le principe organisateur de cette modernité est la constitution de réseaux qui servent aussi bien à se connecter qu'à se déconnecter [54]. Ces évolutions engendrent un état d'incertitude et d'insécurité non pas exclusivement physique, mais plutôt ontologique, cognitive et relationnelle, entraînant une accélération de l'inconfort, du doute, des peurs et de la suspicion qui peut donner lieu à des nouvelles formes de violence individuelle, symbolique et collective. Dans ce contexte, les « *forces de liquéfaction* » de la modernité font émerger un nouveau type de surveillance que Bauman qualifie de « *post-Panoptique* » qui, contrairement au Panoptique de Bentham lu par Foucault, est dynamique, délocalisée, atemporelle et qui repose sur les nouvelles technologies d'information et de protection [55]. Elle affecte tout autant le visible que le virtuel, notamment à travers la surveillance des réseaux d'information et de communication comme l'Internet et la téléphonie mobile. Pour Bauman, cette tendance s'inscrit dans la constitution d'une « *modernité de logiciels* [56] » qui génère une demande croissante d'information portant sur les activités des individus dans la sphère publique et la sphère privée.

L'émergence de nouveaux risques et incertitudes

Ces évolutions s'inscrivent également dans la transformation du concept de risque que la technologie est censée gérer, ce qu'elle s'avère incapable de faire,

52 . *Liquid modernity, op. cit*. Bauman a ensuite poursuivi sa problématique de la liquéfaction dans *Liquid Love, op. cit*., et *Liquid Life*, London, Polity Press, 2005.
53 . La démonstration de Bauman ne se fonde pas seulement sur la technologie et le Panoptique. Elle s'appuie également sur la modernité industrielle (le fordisme), le travail, le lien social, l'identité la politique et la vie de tous les jours.
54 . Pour l'émergence d'une société de réseaux voir aussi Dillon M., « Network society. Network-centric warfare and the State of emergency », *Theory, Culture and Society,* vol.19, n°4, août 2002.
55 . *Op. cit.*, pp. 9-15.
56 . « *Software-based modernity* » dans le texte.

générant de nouveaux risques et incertitudes. Pour Ulrich Beck, la conception traditionnelle du risque reposait sur une idée progressiste de la modernité appelée « *première modernité* » fondée sur le principe qu'« *on pouvait construire des objets et des mondes techniques sans conséquences inattendues* [57] ». Sous l'influence des perspectives dominantes du scientisme, qui excluent toute forme de rationalité autre que la rationalité instrumentale chère à Weber, ce sont les experts techniques qui définissaient le risque et déployaient des techniques rationnelles de probabilité et de calcul pour prévoir les risques attendus [58]. Toutefois, l'évaluation du risque est subjective et le langage employé par les experts peut manipuler le public au lieu de l'informer. Pour Beck, dans la nouvelle phase de la modernité appelée « *modernité réflexive* », « *quoi que nous fassions nous nous attendons à des conséquences inattendues* [59] » car il est impossible d'imputer les risques à des causes externes. A l'instar des dangers écologiques, les nouveaux risques sont produits par la société moderne elle-même. Dans ce contexte, il est possible de se demander si le terrorisme fait partie de ce type de risques. Beck distingue entre les risques « *qui font partie de la "société mondiale du risque"* », comme les dangers écologiques et économiques et les nouvelles menaces terroristes dont on prend conscience. Si les premiers doivent être compris comme conséquences secondaires non voulues d'actions intentionnelles, selon lui, les nouvelles activités terroristes se présentent quant à elles comme des « *catastrophes délibérément provoquées* [60] ».

Toutefois, dans cette nouvelle phase de la modernité, le risque et l'incertitude sont des constructions sociales. Echappant à la quantification, ils sont déterminés en faisant appel à des jugements culturels stéréotypés qui jouent un rôle décisif dans leur perception [61]. La technologie participe à la désignation des risques mais, en même temps, elle en crée de nouveaux car

> « plus l'anticipation des conséquences est intégrée aux systèmes techniques, plus il est manifeste que nous perdons irrémédiablement le contrôle. Toutes les tentatives faites pour minimiser ou supprimer les risques à l'aide de la technologie ne font que décupler l'insécurité dans laquelle nous entraînons le monde [62] ».

Ainsi, selon Beck, la science et la technologie qui « *ajoutent leurs incertitudes aux incertitudes générales au lieu de les minimiser* [63] » ont pour conséquence de rendre la modernité plus aléatoire.

---

57 . Beck U., *Pouvoir et contre-pouvoir à l'heure de la globalisation*, *op. cit*., p. 207.
58 . Pour ces techniques et en particulier l'apport des mathématiques voir Dupuy J.-P., *Pour un catastrophisme éclairé*, Paris, Seuil, 2002.
59 . *Ibid*.
60 . Beck U., *op. cit*., p. 184.
61 . *Ibid*., p. 214.
62 . *Ibid*., p. 207.
63 . *Ibid*., p. 208.

L'accélération du phénomène de privatisation de la sécurité

Parmi les éléments du contexte, la privatisation de la sécurité s'inscrit dans la dynamique du retrait progressif de l'Etat de certains services publics comme l'énergie, les télécommunications, la sécurité et l'ouverture croissante de ces secteurs à des entreprises privées. Selon Frédéric Ocqueteau, les politiques de privatisation adoptées dès les années 1970 sous la vague des politiques néolibérales résultent de la conjugaison de trois phénomènes : la crise fiscale des Etats-providence ; la baisse relative des allocations de ressources publiques en matière de sécurité ; l'idéologie de l'Etat minimal ou de la sortie de l'Etat providence qui permet l'emprise croissante d'un secteur marchand prestataire de services de protection et de sécurité [64]. Toutefois, il convient de rappeler qu'il ne s'agit pas d'un transfert total des fonctions de protection de l'Etat au secteur privé, mais d'une délégation contrôlée de certaines fonctions comme les travaux de Recherche et Développement (R&D), l'exploitation des réseaux de communication, la production des titres d'identité, l'impression fiduciaire, la protection des bâtiments, le contrôle des titres dans les transports publics, etc. Ce phénomène a contribué à la progression rapide d'un marché de technologies de surveillance et de protection dont le chiffre d'affaires a doublé depuis les années 1990. Ce marché a également bénéficié des législations adoptées en matière de sécurité. En France par exemple, l'Etat a validé la privatisation d'une partie des missions de sécurité par la loi d'orientation et de programmation sur la sécurité de 1995, en reconnaissant le gardiennage, la vidéosurveillance, les audits et les conseils en gestion du risque comme des activités participant à la production de la sécurité collective. Cet « encouragement » s'est poursuivi avec l'émergence d'un secteur de fabricants d'équipements de protection qui s'est spécialisé dans le déploiement des techniques biométriques et de surveillance pour la protection des biens publics et privés. Dans le même temps, on a vu apparaître un secteur de services portant sur les activités dites de « prévention des risques » qui, pour Frédéric Ocqueteau, a abouti à la mise en place d'un dispositif de savoir-pouvoir visant la diminution des comportements à risque [65]. Reposant sur les technologies de surveillance de proximité ou à distance et des logiciels de détection de comportements criminels, ce dispositif a contribué à faire des technologies émergentes un instrument incontournable de prévention des risques et des dangers pour les forces de l'ordre.

La mise en place d'une surveillance globale incitée par les Etats-Unis.

Les attentats du 11 septembre et la guerre contre le terrorisme déclarée par l'administration Bush ont accéléré et renforcé le processus de sécurisation entamé depuis la fin de la Guerre froide. Désormais, la sécurité a été érigée

64 . Ocqueteau F., *op. cit*., p. 19.
65 . *Ibid*., p. 14.

par les Etats-Unis comme la préoccupation principale mondiale et les dispositifs de surveillance et d'identification ont acquis une dimension structurante dans les relations internationales. Ainsi, à l'instar des techniques biométriques exigées pour les visas et les passeports afin d'entrer sur le sol américain, ces dispositifs, devenus norme internationale, participent à la constitution d'un nouveau régime de contrôle des identités et des mouvements.

Les politiques de sécurisation adoptées depuis le 11 septembre et renforcées à la suite des attentats de Madrid et de Londres ont permis l'apparition de quatre espaces de surveillance où les technologies nouvelles sont appelées à identifier et anticiper les menaces. Ces espaces sont les frontières (terrestres, maritimes et aériennes), l'espace public (la place publique et les institutions publiques), la sphère privée (le monde vécu) et l'espace communicationnel et virtuel (la téléphonie et l'Internet). Nous ne pourrons pas développer ici l'usage des technologies de sécurité dans chacun de ces espaces, mais nous dirons que le déploiement transversal des techniques d'identification, de surveillance, de traçabilité, de profiling, d'anticipation de risque, etc., a donné lieu à la mise en place d'une surveillance dématérialisée et intrusive dont l'objet focal est l'individu, et l'outil stratégique toute information se rapportant à lui. Depuis 2001, ce dispositif a été renforcé et globalisé par un jeu de coopération forcée et d'émulation entre les Etats-Unis et l'Union européenne laquelle, malgré les réticences du Parlement européen, s'est alignée sur la politique de surveillance et de contrôle imposée par l'administration américaine. Il convient également de rappeler le rôle de plus en plus contraignant de l'OACI dans la fixation des normes internationales d'identification et de voyage [66].

Cette évolution suscite un certain nombre de craintes portant sur la protection des droits fondamentaux, dont en particulier la liberté de mouvement et la protection des données personnelles [67]. Elle suscite également des inquiétudes au regard de la perte de la souveraineté des Etats face à un dispositif technologique imposé par les Etats-Unis. Cette question doit être appréhendée dans le cadre de la problématique plus générale de la globalisation de la surveillance [68]. Selon Ulrich Beck, qui récuse le principe d'incompatibilité entre la souveraineté étatique et la globalisation, la coopération transnationale en matière de sécurité (la coopération militaire, policière, juridique et technologique) comme toute autre coopération interétatique conduit certes à une diminution de l'autonomie nationale des Etats, mais pas à une perte de souveraineté. Car :

66 . *Ibid*.

67 . Cette question a donné lieu à d'importantes publications. Voir entre autres « Défense et identités : un contexte de sécurité global », *Cultures & Conflits*, n°44, 2002 ; « Suspicion et exception », *Cultures & Conflits*, n°58, 2005 ; Herschberg E., Moore K.W., *Critical Views of September 11*, SSRC, 2006.

68 . Voir Sheptycki J., *En quête de police transnationale, vers une sociologie de la surveillance à l'ère de la globalisation*, Bruxelles, Larcier-De-Boeck, 2005.

> « si on juge la souveraineté à l'aune du pouvoir de réalisation politique […] alors la hausse des interdépendances et de la coopération, c'est-à-dire la perte de l'autonomie, débouche sur un gain de souveraineté réelle. Bref en se partageant et en s'associant, la souveraineté ne s'amoindrit pas, au contraire : le partage décuple la souveraineté de chaque Etat [69] ».

Cette position nous paraît néanmoins problématique. On peut certes assumer que dans une optique contractuelle, la coopération interétatique n'annule pas la souveraineté quand elle laisse la possibilité à un Etat de se retirer quand il le souhaite. On peut également parler des bénéfices de la coopération dans une optique européenne où les Etats partagent leur souveraineté pour garantir l'effectivité de celle-ci en la déléguant à une autorité supranationale [70]. Toutefois, la coopération transnationale en matière de lutte contre le terrorisme ne laisse pas aux Etats la possibilité de se retirer à chaque moment car, si un Etat refuse de se conformer aux normes techniques et sécuritaires édictées par les Etats-Unis en matière d'identification, ses ressortissants ne pourront plus entrer sur le sol américain. Ainsi, les Etats sont obligés de se plier aux normes techniques (biométrie), à la liste de personnes interdites d'entrée aux Etats-Unis (*No-Fly List*) et aux PNR [71] sans possibilité de recours ni liberté de choix. La coopération ne permet pas non plus l'émergence d'une structure supranationale qui gère le régime international de mouvements. L'OACI, même si elle est un organisme de l'ONU, ne semble pas jouir d'une autonomie vis-à-vis des Etats-Unis. Par conséquent, on peut dire que la coopération transatlantique en matière de sécurité correspond plus à une relation forcée (« vous êtes avec nous ou contre nous ») que contractée.

La diffusion du paradigme technologique dans la vie quotidienne (dynamique de confort)

Comme nous l'avons indiqué, dans son interaction avec l'environnement, la technologie au sens de dispositif crée un mode de vie, des contraintes et de nouvelles habitudes et conduites. Cette caractéristique a pris une dimension plus extensive avec la globalisation dont une des conséquences est l'intrusion croissante du « *paradigme technologique* » dans la vie de tous les jours. Appelé « *effet de diffusion* », ce phénomène est généré, selon Manuel Castells, par la constitution de réseaux, la connectivité et la flexibilité propre aux nouvelles technolo-

69 . Beck U., *Pouvoir et contre-pouvoir*, *op. cit.*, p. 187.
70 . Pour plus d'approfondissements, voir Laidi Z., *op. cit*., pp. 31-32.
71 . *Passenger Name Record* : ce sont des informations qui portent sur les caractéristiques personnelles (itinéraires, goûts, préférences) des passagers. Elles sont enregistrées et stockées sur une base de données constituée et gérée par des organismes privés créés par des compagnies d'aviation. Au sujet de l'utilisation par l'administration américaine pour le contrôle des étrangers et la lutte contre le terrorisme, voir Mitsilegas V., « Contrôle des étrangers, des passagers, des citoyens : surveillance et antiterrorisme », *Cultures & Conflits*, n°58, 2005, pp. 155-181.

gies [72]. Selon cet auteur, les réseaux constituent « *la nouvelle morphologie sociale de nos sociétés* [73] », ils transportent la science et la technique sans médium et participent à la mutation des technologies.

Bien que les thèses soutenues par Castells demandent un examen critique, notamment à cause de leur éviction de la politique en dehors du champ de production des rapports sociaux et économiques [74], nous retiendrons ici la notion d'effet de diffusion pour caractériser l'extension rapide des nouvelles technologies du champ des sciences à la vie de tous les jours. Cette notion nous paraît pertinente pour analyser l'acceptation des technologies de sécurité par les utilisateurs privés et l'opinion publique. En effet, dans leurs usages quotidiens, ces technologies ne sont pas exclusivement perçues sous leur aspect sécuritaire, mais sont considérées comme des « technologies de confort » participant à l'amélioration de la vie quotidienne. Elles sont à la fois des technologies de sécurité et des technologies de confort. Pour illustrer ce caractère dual, prenons comme exemple les empreintes digitales. Pendant longtemps, celles-ci ont été acceptées comme une technique d'identification policière employée dans la résolution des affaires criminelles. Or, de nos jours, dans une logique de sécurité alliée à une logique de confort, cette technologie fait partie intégrante des objets de l'environnement immédiat et pratique. Ainsi la retrouve-t-on dans les clés USB, les ordinateurs, les voitures, les portes d'entrée, etc. L'évolution du marché de la biométrie confirme d'ailleurs cette tendance. Selon les chiffres avancés, le marché grand public des empreintes digitales se développe plus rapidement que le marché institutionnel, comme les forces de l'ordre. En 2004 plus de 2,4 millions de capteurs d'empreintes digitales auraient été vendus via des ordinateurs portables, des assistants personnels, de la téléphonie mobile, etc., et ce chiffre a doublé en 2005 [75]. Il convient également de noter que l'aspect pratique des empreintes digitales n'est pas seulement un argument commercial. Selon Pierre Piazza, les discours policiers insistent depuis longtemps sur la dimension de confort afin de mieux faire légitimer et accepter les technologies d'identification par les opinions publiques [76]. Aujourd'hui, cet argument fait encore partie des éléments de justification avancés par les pouvoirs publics pour faire accepter la future carte d'identité biométrique dite « carte INES », comme une carte de services utile pour faciliter les échanges dématérialisés par sa fonction de certificat d'authentification [77].

---

72 . Castells M., *The Rise of Network Society*, traduction française : *La Société en réseaux. L'ère de l'information*, Paris, Fayard, 1998, p. 43.

73 . *Ibid*., p. 525.

74 . Voir les critiques de Musso P., « Genèse et critique de la notion de réseau », in Parrochia D. (dir), *Penser les réseaux*, Paris, Champ Vallon, coll. « Milieux », 2001, pp. 194-217.

75 . Chiffres avancés par Bernard Didier, directeur scientifique et de développement des affaires division sécurité de SAGEM. Voir *La Biométrie. Compte rendu de l'audition publique du jeudi 4 mai 2006*, Assemblée Nationale, Office Parlementaire d'évaluation des choix scientifiques et technologiques, p. 26.

76 . Piazza P., « Septembre 1921 : la première "carte d'identité des Français" et ses enjeux », *Genèses*, n°54, 2004.

77 . Ceyhan A., « Identité et identification au prisme de la biométrie », www.ihej.org/ressources/ceyhan_20_03_06.

Comme exemple de technologie de confort utilisé à titre de dispositif de surveillance, signalons le téléphone portable, devenu un objet incontournable de la vie quotidienne. Comme on le sait, il est déjà transformé en moyen de traçage des communications et des itinéraires et ne suscite que quelques résistances venant seulement de personnes qui ne souhaitent être ni identifiées, ni localisées. Et pourtant, selon les projets de sécurisation des voyages qui sont en cours d'étude, dans peu de temps, le téléphone portable muni d'empreintes digitales deviendra l'outil d'identification et de surveillance par excellence des passagers prenant un avion [78]. Comme instrument d'identification, les empreintes digitales serviront d'identifiant pour les contrôles aux frontières. Le téléphone mobile sera porteur de la carte d'embarquement et réceptionnera les informations utiles au moment adéquat (avion retardé, changement de porte d'embarquement, etc.). Comme outil de surveillance, il transmettra les informations concernant les mouvements de l'individu via infrarouge au système de navigation.

Nous pouvons donc dire que le caractère dual des technologies de sécurité témoigne de la généralisation d'une conception de la sécurité en termes de bien, traité selon les principes économiques [79]. Ainsi, avec la prolifération des nouvelles technologies, la sécurité se transforme de plus en plus en un bien qui peut être acheté et vendu sur le marché comme tout autre produit. En tant que tel il peut être quantifié et mesuré à partir de son efficacité et ses coûts. Cette évolution entraîne une pratique non répressive de la sécurité, basée sur le contrôle social et l'autocontrainte qui responsabilisent l'individu. L'individu devient ainsi le gestionnaire de sa sécurité ainsi que de celle de son environnement immédiat.

Les rapports Etat / entreprise

Comme nous l'avons déjà rappelé, le rôle de l'Etat ne s'affaiblit pas au profit d'autres acteurs qui participent à la technologisation de la sécurité. Son action et sa légitimité dépendent de sa capacité à traiter et à coopérer avec eux dans le cadre d'une gouvernance libérale. C'est dans ce cadre d'intelligibilité qu'il convient d'appréhender ses rapports avec les entreprises.

Le processus de coopération Etat/entreprise a commencé dans un premier temps par des politiques de « *spin-off* » qui permettent le transfert des technologies militaires vers le civil dans un souci d'allégement budgétaire. Cette dynamique a permis au secteur industriel de réintégrer les contraintes que le monde militaire subissait depuis longtemps. Sur le plan des techniques, elle a

78 . « Bienvenue dans l'aéroport du futur », Paris Aéroports (magazine des aéroports de Paris), n° 12, juillet-août 2006, p. 73.

79 . Sur la sécurité comme bien, voir Ocqueteau F., *Polices entre Etat et marché, op. cit*, p. 17. Pour une discussion, voir Foessel M., « La sécurité : paradigme pour un monde désenchanté », *Esprit*, août-septembre 2006, pp. 194-208.

permis aux industriels de découvrir le concept de « *systèmes intégrés* » développés par les militaires. Dans un second temps, le processus a été accéléré par des politiques de « *spin-on* » privilégiant les avancées technologiques commerciales et leur exploitation sur le marché de la défense et de la sécurité [80].

Désormais, la tendance en Europe est à la création d'une industrie de sécurité autonome qui développe et commercialise elle-même ses technologies. Non seulement les industriels, mais aussi les responsables de la défense et de la sécurité émettent le souhait de constituer une industrie des technologies de sécurité forte et compétitive sur le plan international. Sur ce point, on remarque que les Etats européens, tout en voulant créer une industrie européenne, sont en même temps préoccupés par la protection de leur propre industrie comme celle des cartes à puce en France. Notons que l'Europe est concurrencée à la fois par les Etats-Unis, mais aussi par la Chine et le Japon où le secteur des technologies de sécurité est en forte croissance, en raison d'un rapide développement des technologies basées sur le RFId [81] insérées dans les cartes à puce. Afin de stimuler son potentiel industriel dans cet environnement concurrentiel, l'Europe a entrepris en 2004 une action préparatoire qui devrait être opérationnelle en 2007 [82]. Cette action prévoit la production de technologies sophistiquées spécialisées pour la surveillance des frontières, l'identification et le traçage des personnes, de technologies de communication et de protection des réseaux, et de technologies de lutte contre le terrorisme.

Quant aux Etats-Unis, l'attitude de l'administration consiste à soutenir les entreprises américaines en suivant une politique plus proche des pratiques de la défense que des pratiques commerciales [83]. On peut observer cette politique dans le soutien au financement des technologies de sécurité par le HSARPA [84]

---

80 . Pour les approches *spin-off* et *spin-on* ainsi que pour la constitution d'un marché de la défense et de la sécurité, voir Versailles D.W., Mérindol Y., Cardot Y., *La Recherche et la technologie, enjeu de puissance*, Paris, Economica, 2003.

81 . RFId : *Radio Frequency Identification*, technologie d'identification par fréquence radio. Elle vise à identifier les objets de tous types en procédant à une saisie de données rapide et automatique grâce aux ondes radio. C'est une technologie de plus en plus utilisée là où d'autres technologies comme les codes barre se heurtent à leurs limites. Elle permet d'attacher son numéro de série de fabrication à l'objet et donc de le repérer de façon singulière. Domaines d'application : 1) Sécurité : marquage de pièces à protéger, sécurisation des processus de production et du processus de transport (par exemple la chaîne frigorifique), 2) Traçage des pièces, 3) Gestion de stocks, 4) Marquage des hommes et des animaux. La CNIL considère que les RFIds sont des identifiants personnels au sens de la loi Informatique et Libertés du fait de leur dissémination massive, de la nature des identifiants de chacun des objets marqués, de leur caractère invisible et des risques de profilage des individus. Voir www.cnil.fr/index.php ?id=1062.

82 . Décision de la Commission concernant la mise en œuvre de l'action préparatoire pour le renforcement du potentiel de l'industrie européenne en matière de recherche sur la sécurité, C(2004)249final.

83 . Voir l'audition de B. Didier, *op.cit*., p.23

84 . *Homeland Security Advanced Research Project Agency*, agence du DHS qui subventionne les technologies de sécurité produites par des compagnies américaines et les labellise.

qui leur attribue le label de « technologies de lutte contre le terrorisme ». On peut aussi l'observer en examinant les donations à certains pays étrangers autorisés à s'équiper en technologies américaines qualifiées.

Dans le processus de technologisation de la sécurité, le rôle des entreprises est double. Elles activent les besoins de la société de confort et participent à la production d'un discours de peur profitant du contexte actuel de problématisation de la sécurité. Sur le registre des besoins de la société de confort, les industriels proposent des produits équipés de technologies de sécurité indispensables dans la vie quotidienne (comme les alarmes, les clés USB, la vidéosurveillance de l'espace privé, etc.). Dans le même temps, beaucoup d'entreprises – accompagnées d'experts – déploient un discours anxiogène portant sur les menaces et risques potentiels en s'appuyant sur tout un matériau statistique et prévisionnel. Dans ce cadre, elles offrent non seulement des produits innovants, mais aussi des logiciels de bases de données accompagnées de méthodes d'évaluation et de gestion de risques. De même, constatant la volonté de la Commission européenne d'approfondir la recherche dans ce domaine, ces mêmes entreprises cherchent à participer aux projets européens comme le programme SAFEE (*Security of Aircraft in the Future European Environment*) [85] dont l'objectif est de placer dans les avions de ligne de nouveaux équipements de sécurité pour lutter contre le terrorisme, à l'horizon 2010-2015. Ces équipements sont essentiellement des caméras et des micros qui observeront les passagers et enregistreront leurs conversations en cabine, des systèmes de reconnaissance numérique de l'iris ou de l'empreinte digitale qui contrôleront l'accès au cockpit et des systèmes d'évitement permettant d'empêcher une collision avec un bâtiment. Au-delà de son aspect technique qui demande une évaluation scientifique spécialisée, cette initiative prévoit la transformation des pilotes de ligne en surveillants qui auront pour mission de surveiller les passagers et de détecter les « personnes à risques » en se connectant au fichier des personnes recherchées. Rappelons que ce type de projet n'est pas nouveau. En France, par exemple, un projet similaire prévoit de confier aux conducteurs des bus de la RATP une véritable mission d'enquête en matière de disparitions d'enfants et de surveillance des pédophiles en les connectant à la base de données des enfants disparus ou enlevés. Même si, pour l'heure, ce type de projets suscite de fortes résistances de la part des conducteurs de la RATP et des syndicats, ils sont néanmoins en cours d'étude.

Finalement, nous pouvons dire que la technologisation de la sécurité opérée dans une gouvernance libérale et une « *gouvernementalité par l'inquié-*

85 . Lancé en 2004 par la Commission européenne, le programme SAFEE lie trente-quatre sociétés aéronautiques comme Airbus, BAE Systems, Thales, Sagem. Son budget est de trente-six millions dont dix-neuf millions pris en charge par la Commission.

tude [86] » soulève des questions éthiques, juridiques, philosophiques, sociologiques et politiques qui prennent un sens particulier dans le contexte de risques et d'incertitudes.

Toutefois, tout en portant sur les rapports entre la technologie et la sécurité, ces questions renvoient à une problématique plus fondamentale qui est celle de la production du vivant et des rapports humains par les progrès techniques. A l'instar de la manipulation des embryons humains et du travail sur le code génétique, ces progrès introduisent un phénomène radicalement nouveau : la technique est désormais capable de modifier fondamentalement ce qui fait de l'homme un homme. Elle est appelée à façonner les relations humaines avec des logiciels, des puces et des nano-objets. C'est dans ce contexte que la technologisation de la sécurité participe à la transformation des rapports humains non seulement dans l'immédiat, mais aussi et surtout avec un impact sur le futur.

Dans ce cadre, sur quelle base fonder l'éthique ? Sur le principe de précaution, sur les seules ressources de la raison humaine ou sur un autre fondement ? Quel pouvoir régulateur lui donner face au développement scientifique et technologique de l'humanité ?

Nombreux sont ceux qui en appellent à la généralisation du principe de précaution comme fondement d'une éthique. Portant sur les risques potentiels [87] , ce principe, qui se présente comme une nouvelle façon de décider face à un avenir incertain, a été développé à l'origine par le philosophe Hans Jonas. Critiquant la vision utilitariste de la nature, Jonas a voulu proposer une « *éthique du futur* » afin de responsabiliser les individus vis-à-vis des effets ultérieurs non voulus de leurs actes bien intentionnés [88]. Dans son usage contemporain, le principe de précaution est appelé quand l'incertitude scientifique retarde la mise en place d'une politique de prévention. Il autorise à prendre des mesures préalables en toute circonstance, même en l'absence de preuve scientifique du lien de cause à effet. Généralement, il est déployé en matière d'environnement et de la santé, mais malgré sa popularité, ses fondements sont l'objet de critiques et de discussions.

Toutefois, bien que ce principe puisse avoir une certaine résonance dans ces domaines son adoption dans le champ de la sécurité soulève un certain nombre de problèmes : le traitement d'un risque environnemental et d'un risque de sécurité relèvent-ils des mêmes fondements et méthodes ? En d'autres termes, peut-on concevoir la sécurité comme un objet naturel ? La prévention

86 . Bigo D., « Sécurité et immigration : vers une gouvernementalité par l'inquiétude », *Cultures & Conflits,* n°31-32, 1998, pp. 13-38.

87 . « Risque potentiel » : ce n'est pas la réalisation d'un danger qui est potentielle, mais le danger lui-même.

88 . Jonas H., *Le Principe de responsabilité. Une éthique pour la civilisation technologique*, Paris, Flammarion, coll. « Champs », 1995.

des menaces de sécurité est-elle du même ressort que la prévention des conséquences de nos actes personnels ? Peut-on appliquer une morale du sens commun qui, selon Jean-Pierre Dupuy, signifie « *ce que l'expérience commune de l'humanité fait tenir pour une évidence commune* [89] » à une question de sécurité ? Doit-on faire appel à une « *heuristique de la peur* », qui pour Jonas implique d'envisager la peur comme instrument de connaissance ? Si oui, vis-à-vis de quoi ? Des risques produits par la technologie ? Des menaces à la sécurité ou des politiques d'exception qui érigent la sécurité comme la préoccupation politique qui surplombe toutes les autres ?

Ces questions en appellent d'autres portant sur les aspects juridiques, philosophiques, sociologiques, politiques et internationaux. Ainsi, sur le plan juridique, doit-on appeler au droit (interne, international et européen) pour réguler l'action publique et privée face aux risques techniques et de sécurité ? Le droit possède-t-il les moyens nécessaires pour être efficace quand on sait qu'en matière de technologies de sécurité ce sont les technologies qui définissent les états de fait et que le droit les régule ensuite ?

Sur le plan philosophique, que devient l'altérité quand l'identité est réduite à la mêmeté ? Comment protéger l'identité ipse face à l'identité rationalisée et catégorisée par la technologie [90] ? Comment restaurer la confiance quand tout devient un risque potentiel ?

Sur le plan sociologique, comment envisager l'impact des technologies de sécurité sur la violence ? La mise en place de nouvelles technologies ne génère-t-elle pas de nouveaux délits et de nouveaux dommages ? Sur quoi fonder une réflexion prospective sur l'éventualité des dysfonctionnements et des conséquences perverses des technologies de sécurité sur les organisations [91] ?

Sur le plan de la science politique et des relations internationales, comment envisager la politique dans ce nouvel horizon temporel marqué par l'incertitude ? Quelle est la place de l'avenir dans les décisions politiques présentes ? Qui a le pouvoir de définir les risques potentiels ? Si, pour Ulrich Beck, la définition des risques appelle à une « relation de définition [92] » au niveau global, quelle coopération établir avec des institutions privées et publiques internationales ? Que devient alors l'Etat quand ses fondements weberiens se voient défiés

89 . Selon Jean-Pierre Dupuy, la morale du sens commun présume que « *1) les actes sont plus importants que les omissions, 2) les effets proches sont beaucoup plus visibles et donc comptent plus, que les effets lointains, 3) les effets individuels ont plus d'importance que les effets de groupe ou effets de composition* ». Voir Dupuy J.-P., « Rationalité scientifique et raison pratique » in *Philosophie, science et éthique, Journée de l'UNESCO*, Editions UNESCO, 2004, pp. 13-14.

90 . Voir l'article suivant dans ce numéro : Ceyhan A., « Enjeux d'identification et de surveillance à l'heure de la biométrie ».

91 . Voir Marx G.T., « Technologies de sécurité et société », *op. cit.*

92 . Beck U., *op.cit*., p. 149.

par la mise en place d'un régime global de surveillance et d'identification décidés ailleurs et avec d'autres acteurs ? Assiste-t-on à une perte de souveraineté ou au contraire celle-ci devient-elle plus efficace ? Dans ce contexte, l'Etat a-t-il la volonté et la capacité d'inventer un système juridique et un environnement politique capables de protéger les citoyens, qui sont de plus en plus démunis face à l'intrusion des technologies de sécurité dans leur vie et à l'émergence d'une multitude d'acteurs gouvernant leur monde vécu sans leur accord ?

Ces questions ne sont certes pas exhaustives, elles montrent cependant combien cette problématique qui ne concerne pas que la *technê*, mais fondamentalement l'homme et son avenir, est multidimensionnelle et demande un examen pluridisciplinaire approfondi.