

Biométrie : les nouvelles formes de l'identité

Michaël Foessel et Antoine Garapon

La biométrie désigne une technologie d'identification et d'authentification qui consiste à transformer une caractéristique biologique, morphologique ou comportementale en une empreinte numérique. Son objectif est d'attester l'unicité d'une personne à partir de la mesure d'une partie inchangeable ou immaîtrisable de son corps¹.

Le recours à des procédures biométriques d'identification constitue l'un des instruments les plus prometteurs de la lutte antiterroriste contemporaine. Notamment aux États-Unis qui l'ont imposé à un certain nombre de leurs partenaires, dont l'Europe. C'est ainsi qu'une carte d'identité biométrique a été décidée en Grande-Bretagne et qu'un projet analogue est très avancé en France. Outre les bénéfices internes (réduction de la fraude à la «carte vitale» notamment), les bénéfices attendus concernent le contrôle de l'immigration et le contrôle des frontières. Ce type de contrôle, réputé inviolable, procure un sentiment de maîtrise sur une sorte de trou noir sécuritaire aux confluent de l'immigration clandestine, du trafic et du terrorisme. C'est ce qui explique son succès et les espoirs qui sont aujourd'hui mis en elle tant de la part des gouvernements que des gouvernés. Comment expliquer autrement la relative passivité des opinions publiques face à un phénomène de plus en plus massif ? Lorsqu'ils sont remis en cause, les usages de la biométrie le sont à partir de leurs effets en général et non en rapport à la lutte antiterroriste². Pour expliquer cette relative inertie des opinions publiques, on fera l'hypothèse que c'est dans la nature du terrorisme contemporain que s'ancre la justification de la biométrie : d'un phénomène à l'autre, c'est toute une logique de l'action sécuritaire qui se met en place.

Menace terroriste et réplique biométrique

La généralisation de la biométrie et des formes d'identification qu'elle permet trouve d'abord sa justification dans l'anonymat caractéristique de l'action (et de l'acteur) terroriste. «Identifier» signifie toujours ramener de l'inconnu à du connu par le moyen de critères relativement stables de reconnaissance. Il faut bien alors admettre que le terrorisme mondialisé n'offre pas de tels critères et qu'il est légitime de chercher à les reconstituer à nouveaux frais. Dans un arrêt récent (dont les conclusions ont été confirmées par les attentats de Londres de juillet 2005), la Chambre des lords notait que les nationaux peuvent se révéler tout aussi dangereux pour la sécurité du pays que les ressortissants étrangers³. Cette fluidité implique que la frontière séparant les «terroristes» du reste de la population est de moins en moins souvent définie sur la base de critères liés à l'appartenance nationale. Priment désormais des clivages traversant les nations elles-mêmes. Dans un contexte où le suspect n'est pas nécessairement un étranger, un nouvel entrant ou même un activiste, émerge la figure de l'«ennemi intérieur» apparemment rétif à toutes les procédures classiques d'identification.

La biométrie semble bien constituer une réponse adéquate et efficace à cet effacement des critères traditionnellement retenus en matière de dangerosité. Les paramètres biométriques identifient, en effet, un individu sans considération de son appartenance nationale ou communautaire et selon des critères qui n'empruntent rien à sa biographie⁴. Et parce qu'elle l'identifie de la sorte, la biométrie permet de le suivre à la trace. La comparaison la plus parlante est probablement celle que l'on peut faire avec le suivi du transport des marchandises suivant le principe de «traçabilité»: il s'agit dans les deux cas d'identifier des individus, de mettre en mémoire leurs itinéraires et de déduire un degré de dangerosité de la nature des mouvements observés. La caractéristique de l'individu (chose ou personne) importe peu, *a fortiori* son identité politique, ethnique ou religieuse. Seuls sont retenus comme efficaces des critères parfaitement objectifs susceptibles de servir d'outils de repérage.

La biométrie s'inscrit donc dans un contexte où «la surveillance devient sans cesse davantage déterritorialisée et intrusive⁵». Mais si le terrorisme contemporain vient légitimer cette mutation dans les technologies de surveillance, c'est bien parce qu'il est lui-même déterritorialisé et intrusif en sorte que terrorisme et reconnaissance biométrique font système. Dans cette logique d'implication mutuelle, il s'agit de faire face à de nouvelles incertitudes qui semblent presque naturellement appeler une riposte de type technologique. Le terrorisme désigne, en effet, une stratégie de l'indiscrimination qui se distribue dans divers registres : confusion entre les civils et les combattants, entre «victimes» et «coupables» et entre public et privé. Ce dernier aspect est décisif pour le problème qui nous préoccupe : phénoménologiquement, l'attentat terroriste manifeste la disparition de la distinction entre le front et l'arrière au profit de lieux indistincts (privés et publics) comme la rue, la bouche de métro ou l'aéroport. La stratégie terroriste est ainsi une stratégie de l'ubiquité : il s'agit de convaincre l'«ennemi» que tout espace peut, à tout instant, devenir un lieu de combat.

Or, il existe une condition nécessaire à la mise en œuvre de cette stratégie : l'anonymat du terroriste. Comme le remarque Dominique Linhardt, le terroriste «se fond dans l'indiscrimination du monde commun» épousant jusque dans ses moindres détails les caractères du civil débonnaire⁶. On peut même dire que le terroriste retourne contre lui-même le principe démocratique de la présomption d'innocence : il a besoin d'apparaître comme «celui qui ne peut pas nuire» pour conférer à son acte le maximum de portée. L'attentat terroriste constitue donc une subversion radicale de la norme à partir de son respect apparent : il s'agit dans tous les cas de faire surgir la terreur depuis un lieu neutre (l'espace commun) et dans un élément *a priori* rassurant (le quotidien) en rendant tout à coup incertains le comportement et l'usage des objets les plus communs (la voiture explose quand on tourne la clé du démarreur, le métro déraile, l'eau est empoisonnée). Cette stratégie est nécessaire à la fois pour rendre imprévisible la survenue de l'acte et incalculables ses effets.

En conséquence, le terrorisme mise sur une stratégie de la visibilité retardée. À l'anonymat et à l'indistinction doit en effet succéder de manière brutale et violente une forme de publicité totale, relayée par les médias. C'est à ce point d'articulation entre dissimulation et visibilité que se situe la biométrie. Cette dernière permet, en effet, d'établir des critères d'identification stables puisqu'ils sont informatisés et encodés dans un langage universel, et permanents puisqu'ils s'ancrent dans la permanence du corps. Le présupposé d'une telle procédure est que le corps est la seule chose dont un individu ne puisse se déprendre à un moment où aucun autre identifiant (culturel, politique ou même biographique) ne résiste à l'indistinction propre à l'action terroriste. C'est donc l'inertie du corps qui est requise comme un rempart aux stratégies de la dissimulation.

Mais de quel corps s'agit-il ? En aucun cas du corps vécu qui ne fournit aucune base fiable de reconnaissance, ni même du corps physique qui est sujet, lui aussi, aux aléas du temps et à la possibilité de la dissimulation. Le corps dont s'occupent les techniques biométriques est un corps paradoxal puisqu'il est tout à la fois objectivé (réductible à des paramètres informatiques) et naturel (inaltérable). C'est même, en toute rigueur, un corps métonymique comme l'atteste l'importance de l'iris comme organe privilégié par la reconnaissance biométrique : cet organe, dont les paramètres biologiques sont inaltérables, désigne un principe de constance.

Une redéfinition des frontières

L'apparition du terrorisme mondialisé n'est aucunement à l'origine de l'usage de la biométrie dans les techniques de sécurité. Plus qu'une rupture, les événements du 11 septembre ont «révélé et accéléré un processus de sécurisation entamé depuis la fin de la bipolarité⁷». De fait, alors que les premières expérimentations datent des années 1950, la biométrie se généralise à partir du moment où les affrontements liés à la guerre froide laissent place à des violences et à des infractions transnationales. Mis à part les cas d'espionnage, la bipolarité traçait en effet une ligne de démarcation nette entre amis et ennemis, la «dangerosité» d'un individu pouvant être induite de son marquage idéologique.

A contrario, il existe un lien très fort entre la dépolitisation des conflits et la technicisation des procédures sécuritaires : la biométrie résulte d'une nouvelle appréhension des frontières et participe d'un renouvellement de leur définition. Les premières politiques biométriques datent du milieu des années 1980, à l'occasion de la « guerre contre la drogue » décrétée par le gouvernement américain. Cette « guerre », qui anticipe sur bien des points la « guerre contre le terrorisme » des années 2000, est un conflit de type transnational : le problème est de lutter contre des mouvements anarchiques de marchandises et de personnes et non contre des groupes localisés et homogènes. Dans ce cadre, la figure du trafiquant se rapproche de celle de l'immigré clandestin : dans les deux cas, l'activité policière se joue à la frontière (en l'occurrence, la frontière entre les États-Unis et le Mexique). On comprend alors pourquoi la frontière est devenue un lieu d'expérimentation privilégié pour les techniques biométriques, avec la mise à contribution de pas moins de 54 agences de sécurité pour surveiller les abords du Texas et de la Californie.

Aux États-Unis, ces nouvelles approches de la surveillance et du contrôle prennent tout leur sens si on les replace dans le cadre de l'*homeland security*, un concept qui repose sur le présupposé (accru depuis le 11 septembre) d'une vulnérabilité du territoire national. Créé en 2003, le Department of Homeland Security marque l'unification institutionnelle de plusieurs agences de sécurité autour d'un même objectif : « La prévention, la dissuasion, la préemption des agressions pouvant être commises sur le sol américain à l'encontre des populations et des infrastructures critiques⁸. »

Bien loin de renforcer le rôle de la frontière comme limite spatiale, l'usage de la biométrie contribue à la « dématérialisation » comme à la « déformalisation » de la frontière. Il ne peut s'agir d'un pur et simple repli sur soi ou d'un retour à l'autarcie qui marquerait une rupture par rapport aux exigences les plus élémentaires du commerce international. À ce titre, les décisions américaines consécutives au 11 septembre concernant la frontière avec le Canada (puis, plus tard, les échanges avec l'Europe) sont tout à fait révélatrices. Pour sécuriser leur frontière nord tout en évitant de mettre leur propre pays en situation d'embargo, les États-Unis ont mis en place, dès le mois de décembre 2001, un ensemble d'accords intitulé *Smart borders*. Ce dispositif décidé en accord avec le Canada généralise précisément l'emploi de mesures biométriques de reconnaissance qui constituent ainsi le socle d'une différenciation entre le « bon étranger » (touriste ou commerçant) et le « mauvais » (terroriste ou trafiquant).

La biométrie permet ce que les mécanismes traditionnels de contrôle à la frontière rendaient impossible, à savoir une anticipation du risque en amont de la frontière. En raccordant des données biométriques (empreinte digitale, iris, voix, etc.) à des banques de données informatiques, l'État se donne ainsi les moyens de déceler des groupes d'individus indésirables avant qu'ils n'atteignent matériellement la frontière. En effet, et ceci est vrai aussi de la France qui utilise la biométrie dans de nombreux consulats en Afrique, le contrôle informatisé se réalise au niveau des ambassades, dans les aéroports ou auprès d'entreprises privées comme les compagnies aériennes. On assiste ici à une inflexion des modalités de la surveillance qui ne s'effectue plus directement mais à distance.

Bien sûr, la biométrie n'est pas à l'origine de ce paradigme de la surveillance à distance. Comme l'a montré Didier Bigo⁹, les agences de sécurité (qu'elles soient publiques ou privées) ont depuis longtemps affaire à des «champs de sécurité» plus qu'à des domaines circonscrits et stables. Les polices de renseignements, en particulier, se distinguent des polices judiciaires par le caractère indéfini et immatériel de leur champ d'action : il s'est toujours agi pour elles de «surveiller à distance» si, par là, on entend le procédé qui consiste à induire la dangerosité d'un individu de sa trajectoire. Mais, avec la biométrie, la surveillance s'édifie sur des principes totalement *a priori*, ce qui suppose encore la constitution d'un système de classification des mouvements en fonction de leur signification présumée.

Avec le contrôle biométrique, la frontière perd son statut de démarcation géographique pour devenir à la fois fonctionnelle et virtuelle. Elle est «déformalisée» au sens où elle ne désigne plus une ligne de partage entre deux espaces et deux souverainetés, mais une zone de contrôle qui doit permettre la distinction entre les individus dangereux et les autres. Cette «zone» tend elle-même à devenir virtuelle, construite exclusivement sur la base de paramètres informatiques. C'est depuis le consulat où il demande un visa que l'étranger est identifié à l'aide de caractérisations biométriques reversées à une banque de données. Cette forme inédite d'identification à distance assure en quelque sorte la transformation de la frontière de ligne en «acte»: c'est l'État qui trace une frontière idéalement infranchissable entre un individu et son territoire et cette frontière débute de manière arbitraire depuis le lieu où se situe l'individu en question.

Plus encore qu'à une globalisation des méthodes de surveillance, on assiste donc à une diffusion du contrôle hors des limites traditionnelles et territoriales de l'exercice de la souveraineté. À l'opposé de sa définition classique, la frontière perd son caractère spatial : elle doit être partout et nulle part comme l'illustre la déterritorialisation des contrôles¹⁰. La biométrie produit une information où chaque individu devient en quelque sorte son propre territoire et elle instaure une géographie du corps humain d'un genre inédit. La frontière n'est plus une réalité physique, géographique : elle est affirmation de la puissance. Elle commence dans la capacité à établir scientifiquement la singularité de chacun pour distinguer ensuite de manière infaillible entre les hommes d'un même territoire. Elle ne suit plus les contours de la géographie mais passe désormais parmi les hommes.

La dépolitisation des identités

La généralisation des procédés de reconnaissance biométrique a donné lieu à de nombreuses interprétations sur la nature du pouvoir dans des démocraties technologisées. Parmi celles-ci, la théorie dominante est incontestablement celle qui lie la biométrie au paradigme biopolitique et fait du traitement informatisé et sécuritaire du corps le signe le plus spectaculaire de l'insinuation d'un pouvoir technologisé dans l'intimité des vies. Dans ce sens, Giorgio Agamben identifie le système de traçage biométrique des individus à un «tatouage biopolitique», un procédé de marquage qui institue une continuité entre les démocraties contemporaines et l'univers concentrationnaire¹¹. La biométrie «autorise l'inscription et le fichage de l'élément le plus privé et le plus incommunicable de la subjectivité¹²» et porte à son terme un processus de capture du corps par le pouvoir. De plus, cette atteinte à l'intime (identifié ici au corps biologique) qui devait être exceptionnelle tend à devenir la norme, illustrant la thèse bien connue d'Agamben selon laquelle l'état d'exception est la véritable source du droit.

Cette critique vise juste dans la mesure où elle dénonce l'identification du politique à la sphère restreinte du bio. Mais l'équivalence qui est ici présumée entre la subjectivité et le corps biologique individuel est sujette à caution. Surtout, il est discutable de prétendre saisir l'essence (biopolitique) du pouvoir à partir de l'une de ses manifestations contemporaines les plus spectaculaires. Faire de la biométrie la vérité enfin dévoilée du pouvoir n'est pas seulement excessif, cela risque d'être aveuglant puisque se trouve alors méconnu le principal effet de cette procédure sur les modalités de la reconnaissance et de la surveillance.

La biométrie, en effet, charrie un concept déterminé de l'identité individuelle et personnelle et c'est ce concept, s'il devait devenir exclusif de tous les autres, qui doit être critiqué. Il faut d'abord noter que la biométrie réalise une forme de dépolitisation et d'individualisation de la surveillance qui se distingue du modèle du «panoptique» défendu autrefois par Michel Foucault. Il ne s'agit plus pour l'État de tout voir sans être vu, mais plutôt de s'immiscer jusque dans les particularités extrêmes de l'existence individuelle pour réduire cette dernière à une somme de paramètres constants et objectivés. Il n'est donc nullement nécessaire de «tout voir», mais plutôt, pour reprendre d'autres formules de Foucault, d'«en voir le moins possible» en privilégiant «une visibilité délivrée de toute charge sensible¹³». La biométrie, comme toute science classificatrice, n'a affaire qu'à des «objets filtrés», c'est-à-dire à des figures et des mouvements. Ce n'est pas l'épaisseur des êtres qui l'intéresse mais la constitution d'un «espace taxinomique de visibilité» qui rend possible le partage des individus selon leur dangerosité. Par cette forme d'abstraction qui la caractérise, la biométrie nous rappelle qu'il n'y a de pouvoir que sur les signes et non sur les corps.

Mais cette réduction du corps à des paramètres informatiques a surtout pour effet de privilégier exclusivement ce que Paul Ricœur appelait l'«identité mêmeté» au détriment de l'«identité ipséité¹⁴». Pour reconnaître cette forme d'identité, «on compare l'individu présent à des marques matérielles tenues pour la trace irrécusable de sa présence antérieure dans les lieux du litige¹⁵». L'identité biométrique est reconstituée à partir d'un système de marques qui se trouve inscrit à même le corps objectivé de l'individu. De ce point de vue, la biométrie identifie le corps à un «invariant relationnel» qui met à l'abri du moindre doute sur les faits et gestes d'un même individu en un temps donné. Le critère de similitude devient parfaitement constant puisqu'il est renvoyé aux structures invariantes du corps. La biométrie accède donc en quelque sorte au principe que la philosophie cherchait vainement du côté de l'ontologie de la substance : celui d'une «continuité ininterrompue».

Le risque est celui d'une totalisation de la personne, de ses faits et gestes, sous la catégorie du «même». On peut bien dire que le contrôle biométrique privilégie la structure sur l'événement en figeant l'identité de l'individu au risque de ce que Ricœur appelle le «dénî du changement». Mais si un corps (objectivé) demeure bien le même, peut-on en dire autant d'un sujet et du danger qu'il représente éventuellement pour un État ? N'y a-t-il pas là une manière de ramener un sujet à des caractéristiques inaltérables qui ne laissent que peu de place à l'appréciation des circonstances particulières ? Ce qui, finalement, devient contestable dans la généralisation des procédures de contrôle biométrique à tous les mouvements, c'est la tentation de construire des paramètres dynamiques (l'identité d'un sujet agissant) à partir de données stables (celles de son corps objectif) comme si l'avenir se laissait toujours déduire du passé.

Le risque est aussi celui d'une perte de maîtrise sur ces données qui prennent leur valeur en voyageant et en se conservant. Le partage de ces données avec d'autres États, qui n'ont pas nécessairement les mêmes scrupules, ni le même souci des libertés individuelles, soulève bien des questions. Une trop grande circulation (notamment avec des entreprises privées de sécurité) les rendrait indestructibles. Si les données biométriques devaient s'avérer à la fois indestructibles et permanentes, elles nous condamneraient à vivre dans un monde immobile et sans refuge. Un paradoxe au siècle de la mondialisation et de la vitesse.

Michaël Fœssel et Antoine Garapon

1. Définition donnée par Ayse Ceyhan lors du séminaire IHEJ/Esprit, le 20 mars 2006.

2. Voir la position de la CNIL sur l'expérimentation des visas biométriques du 20 décembre 2004 (www.cnil.fr).

3. Décision de la Chambre des lords du 16 décembre 2004.

4. Bien plus, et comme on le verra, c'est la biométrie qui doit contribuer à la reconstruction des biographies.
5. Ayse Cehan, «Sécurité, frontières et surveillance aux États-Unis après le 11 septembre 2001», *Cultures et conflits*, 53, automne 2004.
6. Dominique Linhardt, séminaire IHEJ/Esprit, 3 avril 2006.
7. A. Cehan, «Sécurité, frontières et surveillance aux États-Unis après le 11 septembre 2001», art. cité.
8. M. Dobbs, "Homeland Security, New Challenges for an Old Responsibility", ANSER Institute for Homeland Security, mars 2001.
9. Didier Bigo, « Gérer les transhumances. La surveillance à distance dans le champ transnational de la sécurité, dans *Penser avec Michel Foucault*, Paris, Karthala/Ceri, 2005, p. 130-160.
10. Sur ce point, voir l'article résolument critique de David Lyon «La frontière est partout : encartement, surveillance et altérité», *Les Cahiers de la sécurité*, 56, 2005, p. 91-106.
11. Voir Giorgio Agamben, «Non au tatouage biopolitique», *Le Monde*, 11 janvier 2004.
12. Agamben, «Non au tatouage biopolitique», art. cité.
13. Voir M. Foucault, les Mots et les choses où ces formules servent à caractériser le système des classifications de l'histoire naturelle à l'âge classique.
14. Paul Ricœur, *Soi-même comme un autre*, Paris, Le Seuil, 1990.
15. Ibid., p. 141.

Revue des revues, sélection de janvier 2007

Michaël FOESSEL & Antoine GARAPON : « Biométrie : les nouvelles formes de l'identité »
article publié initialement dans *Esprit*, juillet-août 2006.

Traducteurs :

Anglais : Ros Schwartz
Arabe : Anouar Moghith
Chinois : Yan Suwei
Espagnol : Claudia Riva-Palacio
Russe : Ekaterina Belavina

Droits :

© Michaël Foessel, Antoine Garapon et *Esprit* pour la version française
© Ros Schwartz /Bureau du livre de Londres pour la version anglaise
© Anouar Moghith /Centre français de culture et de coopération du Caire – Département de
Traduction et d'Interprétation pour la version arabe
© Yan Suwei/Centre culturel français de Pékin pour la version chinoise
© Claudia Riva-Palacio /Institut français d'Amérique latine pour la version espagnole
© Ekaterina Belavina /Centre culturel français de Moscou pour la version russe