Introduction

« Si Marx revenait aujourd'hui, quel phénomène retiendrait-il pour caractériser notre société ? Ce ne serait plus le capital ni le capitalisme mais le développement de la technique, le phénomène de la croissance technicienne »[1]. Les technologies de contrôle se situent dans la prise en compte des techniques et des outils, dont l'importance a commencé à apparaître dès le XIX^e^ siècle, mais qui a donné lieu à un épanouissement littéraire dans les années 1930-1980. Il convient de citer notamment Jacques Ellul, professeur de droit à la faculté de Bordeaux, surtout connu comme historien du droit et sociologue. Commentateur de l'essor du capitalisme, personnaliste, Jacques Ellul considère l'outil technique comme étant au cœur de la société. Le « système technicien »[2] d'Ellul met au cœur du capitalisme techniciste l'aliénation. Chez Ellul, l'outil et la machine sont bien singularisés. Ils jouent un rôle essentiel dans l'économie et le corps social. L'influence des idées d'Ellul a dépassé les frontières françaises pour gagner les Etats-Unis. L'importance de la machine est perçue depuis longtemps. Elle est reconnue au moment de l'avènement de la classe ouvrière et de la bourgeoisie. Elle accompagne la croissance des services et l'innovation. Elle se concrétise dans les inventions et dans le droit de la propriété industrielle, avec ses conventions internationales[3], avec les analyses stratégiques auxquelles procèdent les sociétés commerciales pour déterminer si certains brevets doivent avoir une portée limitée, dans un ou deux États ou un dimensionnement qui s'étend à de nombreux pays. Les machines sont souvent mobiles ; elles sont presque toujours mobiles à partir de 1980 et surtout à partir du XXI^e^ siècle et participent à un contrôle dont les utilisateurs ne sont pas toujours conscients ou à l'égard duquel ils adoptent une attitude

1. Jacques Ellul, « Entretien avec Jean-Claude Gillebaud », *Le Nouvel Observateur*, 17 juillet 1982.

2. Jacques Ellul, *Le système technicien*, Calmann-Lévy, Cherche-midi, Paris, 3^e^ édition, 2012.

3. Convention de l'Union de Paris, Convention PCT, Convention de Munich.

d'indifférence. C'est ce qui apparaît dans le « profilage des populations »[4] qui décortique, analyse les contours et la dynamique de la surveillance post-orwellienne et, parfois, de la cybersurveillance.

Nous sommes entrés depuis plusieurs décennies dans l'ère du numérique. Le numérique concerne quasiment tous les outils, toutes les machines. Le développement passe par le numérique. Dans le secteur des communications électroniques, où l'audiovisuel se conjugue aux télécommunications et à l'informatique, le numérique est le maître-mot. En France, la loi sur le numérique de 2016 a été l'une des plus importantes contributions législatives du gouvernement Valls et avait été précédée d'une consultation des différents acteurs. Le très haut débit est un objectif poursuivi par les états et les entreprises. Beaucoup de nations de l'Europe de l'Est, y compris celles qui appartenaient autrefois au COMECON, ont mis l'accent, avec succès, sur la croissance de la fibre optique, pour compenser le retard pris à l'époque du triomphe de la paire de cuivre dans l'Europe de l'Ouest. La Lituanie venait en tête de liste des états européens en 2014 et 2015 pour la pénétration de la fibre optique, sous sa forme plastique ou comme fibre de verre, alors que le Royaume-Uni et l'Allemagne, où la paire de cuivre avait permis le déploiement de réseaux exhaustifs étaient hors classement. Ce qui est vrai pour la Lituanie l'est aussi pour l'Estonie, la Pologne, la Russie (hors Union européenne), voire la Biélorussie. L'Union européenne a établi un plan de croissance du très haut débit qui est censé se finaliser en 2020, ce qui semble optimiste. Des fonds européens ont été dégagés puis réduits en raison du déficit de la dette qui concerne presque tous les états européens. Les subventions publiques étatiques sont mieux acceptées par la commission lorsque le pays concerné appartient à l'ancien bloc soviétique, qui s'est converti à l'économie de marché depuis 25 ans que dans des états appartenant à la sphère libérale depuis longtemps. En ce qui concerne les mobiles, alors que les chercheurs ont beaucoup progressé sur la 5G, la majorité des entreprises opérateurs privés de télécommunications exploitent les licences de 4G dans le monde développé. Le numérique est facteur prééminent de croissance, mais la fracture numérique est toujours une réalité en Afrique, pourtant présentée comme continent privilégié pour le développement et cette fracture, en matière de fibre optique apparaît entre les zones très urbanisées et les zones à moyenne densité ou à faible densité. La question se pose parfois de savoir si les collectivités territoriales peuvent être partie prenante dans cette partie d'échecs. En France, depuis la LCEN[5],

4. Armand Mattelart, André Vitalis, *Le profilage des populations*, La Découverte, Paris, janvier 2014.

5. Loi pour la confiance dans l'économie numérique du 21 juin 2004, qui transpose la directive du 8 juin 2000 sur le commerce électronique et traite aussi de la cryptologie, au demeurant essentielle pour le commerce électronique et des collectivités territoriales dans le secteur des communications électroniques.

les collectivités territoriales peuvent non seulement développer des réseaux, ce qui était accepté par le Code général des collectivités locales depuis 1999, mais être opérateurs de réseaux. En France aussi, des collectivités locales se sont vu attribuer des licences WIMAX. Mais le même choix n'a pas été opéré dans tous les pays de l'Union européenne, qui, dans une optique néo-libérale nourrissent une méfiance argumentée à l'égard de la participation de collectivités publiques, fussent-elles des régions, à l'exploitation des réseaux, voire des services de communications. Le traité sur le fonctionnement de l'Union européenne, à la suite des précédents traités qui l'ont constituée, affecte une réserve raisonnée et argumentée à l'égard des services d'intérêt général, qui seraient censés constituer une exception dans le paysage technique et économique, pas seulement celui du numérique, mais celui des autres technologies susceptibles de donner une impulsion au marché et à la concurrence.

Le numérique est un facteur dominant dans les technologies qui nous façonnent et que nous gouvernons (à moins que ce soient elles qui nous gouvernent). Les nanotechnologies, les technologies qui conditionnent l'essor de l'environnement, qu'il s'agisse des techniques auxquelles il est fait recours en matière d'énergies renouvelables ou des technologies qui traitent des diverses formes de l'écosystème, sous sa forme végétale, minérale, animale, se combinent au numérique pour se concilier les échanges commerciaux entre pays anciennement ou récemment industrialisés, entre pays émergents, pas seulement les BRICS, mais aussi l'Indonésie, la Corée du Sud, le Mexique, la Turquie, l'Arabie Saoudite, états qui appartiennent tous au G20, entre pays en cours de développement ou encore sous-développés, mais avec des zones d'investissements qui permettent des retours financiers intéressants et rentables. Les techniques, alliées souvent aux services sont donc bien, comme le prétendait Ellul, au cœur d'un système qui a un dimensionnement certes économique, mais aussi juridique, avec un fort souci de rationalisation juridique et géopolitique, puisque les systèmes technicistes passent aussi par un dimensionnement militaire, avec des satellites et des drones qui cultivent aussi bien l'aspect civil et commercial que l'aspect militaire, en connexion avec un complexe militaro-industriel qui n'est pas seulement celui des Etats-Unis et avec des alliances où les Etats-Unis continuent à jouer un rôle déterminant et prédéterminant, dans le cadre de l'OTAN, notamment et avec le concours d'états qui ne sont pas membres de l'OTAN, mais qui comptent sur l'assistance de l'OTAN dans les différends multi-dimensionnels qui les opposent à d'autres entités, états, organisations internationales, lobbies, entreprises diverses et diversifiées.

Les techniques et technologies qui viennent d'être mentionnées donnent lieu à exploitation dans une logique de rentabilité commerciale mais elles concourent également au maintien de la sécurité nationale et de l'ordre public. En fait, elles sont

porteuses de potentialités en matière de surveillance et de contrôle. Ainsi, pour ce qui concerne le secret de la correspondance, les plis courriers pouvaient donner lieu à une ouverture et une lecture dans le cadre des cabinets noirs au XIX^e^ siècle. Dans *Lucien Leuwen* de Stendhal, la capture du télégraphe permet de faire une élection. A la fin du XX^e^ siècle, le téléphone fixe permet des écoutes dans le cadre de la légalité. Avec l'arrivée de l'ordinateur et du téléphone mobile, il est beaucoup plus facile aux citoyens de communiquer entre eux ; il est plus facile aussi à l'état de procéder à de multiples interceptions par le biais des conversations, des courriels, des SMS. Les matériels sont moins chers et les procédés d'interceptions sont moins coûteux. A la fin du XX^e^ siècle, les opérateurs qui procédaient à des interceptions prévues par la loi entraient souvent en conflit avec le ministère de l'Intérieur et le ministère de la Justice, car ces interceptions, qui correspondaient à un service public, paraissaient insuffisamment payées à ces personnes morales de droit privé, tant aux Etats-Unis que dans les autres pays développés. Les pouvoirs publics, eux, qui ont dans leurs missions régaliennes la défense de l'argent du contribuable et des deniers publics se trouvaient dans une logique opposée et les négociations étaient âpres et difficiles.

Au XXI^e^ siècle, le prix d'une interception est beaucoup moins élevé et le nombre des interceptions ne cesse de s'accroître. La recherche du profit est identique pour les sociétés commerciales, mais comme le contexte est moins rigide, les négociations entre opérateurs qui travaillent pour le compte de l'état et l'état sont moins difficultueuses. Avec les interceptions de communications électroniques, nous sommes dans un secteur technologique qui a progressé mais où les procédés d'interceptions étaient une réalité depuis fort longtemps.

D'autres technologies ont, au même titre que les interceptions, connu un essor au XXI^e^ siècle, tout en ayant participé à la défense de l'ordre public au XX^e^ siècle, voire au XIX^e^ siècle. La robotisation et le remplacement de nombreux hommes par des machines intelligentes participent à cette logique. En revanche, d'autres procédés de surveillance et de contrôle sont apparus au XXI^e^ siècle et s'ajoutent à la panoplie déjà existante. Parmi les technologies existant antérieurement mais qui ont connu un essor exponentiel au XXI^e^ siècle, il convient de citer la biométrie et la vidéosurveillance.

La biométrie a d'abord été anthropométrie[6]. Les empreintes digitales existaient déjà au XIX^e^ siècle. Au XX^e^ siècle, une distinction s'est opérée entre biométrie morphologique et biométrie comportementale, qui n'aurait eu aucunement sa place dans les limbes de l'anthropométrie. De même, le taux de faux rejets et le taux de fausses acceptations qui ont pour objectifs de mesurer la fiabilité d'un procédé

6. Berthillon.

biométrique[7] est une émanation du XX^e^ siècle. Parmi les procédés biométriques, l'empreinte digitale, la reconnaissance par l'iris et la rétine sont très fiables. L'empreinte digitale est actuellement le procédé biométrique auquel il est fait le plus souvent recours pour défendre l'état confronté à l'exigence de liberté de circulation avec les visas et les passeports qui se sont unifiés au niveau de l'Union européenne ; l'empreinte digitale trouve aussi sa place dans les aéroports au sein des zones réservées et sur les lignes sensibles, comme celles qui sont à destination de Tel-Aviv. La reconnaissance par l'iris a donné lieu à un brevet aux Etats-Unis, mais ce brevet est à présent dans le domaine public, même si la reconnaissance par l'iris, non seulement pour des raisons tenant à la propriété industrielle, mais à la culture, est plus utilisée aux Etats-Unis qu'en Europe. Les iris de jumeaux monozygotes sont différents et le taux de faux rejet/fausse acceptation est infime. Par ailleurs, l'accès à l'iris ne pose pas de problèmes particuliers aux sujets concernés. La reconnaissance par la rétine est aussi fiable que la reconnaissance par l'iris, mais implique l'assistance d'un ophtalmologue et le recours à la reconnaissance rétinienne se restreint à un univers carcéral. La reconnaissance palmaire, qui, elle, permet de procéder à une image en 3D de la paume de la main, est assez fiable, mais moins fiable que l'empreinte digitale ou la reconnaissance par les yeux. Néanmoins, elle connaît un grand succès dans la plupart des pays développés, car elle n'est pas intrusive et permet de contrôler l'accès aux cantines, destinées aux adultes, aux adolescents, aux enfants et le respect des horaires de travail dans les entreprises[8]. La reconnaissance faciale est moins fiable mais est plus utilisée aux Etats-Unis qu'en Europe. Pourtant, il a été démontré aux Etats-Unis, du fait de confusions entre délinquants et délinquants supposés proclamés par la suite innocents que la fiabilité était moindre que celle de l'empreinte digitale. Aux Etats-Unis, elle a souvent encouru un certain succès à l'occasion de grandes réunions. Aux Etats-Unis et dans la plupart des pays de l'Union européenne, la reconnaissance faciale est couplée à la vidéosurveillance lors d'évènements sportifs. La biométrie comportementale est en général considérée comme moins fiable que la biométrie morphologique. Les techniques de biométrie comportementale sont diversifiées, avec la reconnaissance vocale, la frappe sur le clavier, la signature biométrique, les silhouettes. La reconnaissance vocale a trouvé une célèbre illustration littéraire avec *Le premier cercle* de Soljenitsyne. Le premier cercle est celui des zeks prisonniers intellectuels chercheurs dont le savoir

7. Le taux de faux rejets correspond à un rejet d'un moyen biométrique qui aurait dû être accepté ; le taux de fausses acceptations correspond à des acceptations de moyens biométriques qui n'avaient pas leur raison d'être.

8. La reconnaissance palmaire est préférable pour l'employeur à un badge, qui est susceptible d'être utilisé par quelqu'un d'autre que le salarié ou le collaborateur auquel il est censé être affecté.

et l'imagination créatrice peut être éminemment utile au régime stalinien. Dans cet ouvrage, il est notamment fait mention des recherches en reconnaissance vocale d'un prisonnier qui se passionne pour son travail, mais a aussi conscience, à ce stade, de ses limites. Le régime veut recourir au système de reconnaissance vocale mis au point par ce zek, mais, dans les années 1950, le taux de faux rejet/fausse acceptation était mauvais et il était inévitable d'emprisonner des « innocents » avec « l'ennemi du régime » recherché. La reconnaissance vocale a connu de grands progrès depuis *Le premier cercle*. Des logiciels ont notamment pu améliorer les performances de la plupart des procédés existant en la matière. Cependant, la reconnaissance vocale, y compris en étant améliorée par des programmes d'ordinateurs est très moyennement fiable. La même affirmation est valable pour la quasi-totalité des techniques de biométrie comportementale. La signature biométrique n'est pas acceptée par la CNUDCI[9] ; elle est rarement entrée dans les mœurs juridiques. Aux Etats-Unis, l'état de Californie la reconnaît et l'admet, mais les particuliers et les professionnels californiens recourent infiniment plus souvent à la signature électronique qu'à la signature biométrique. L'empreinte génétique peut être rattachée à la biométrie morphologique, mais d'autres distinctions la classent à part.

Contrairement à une idée courante, l'empreinte génétique n'est pas fiable à 100 %. Mais c'est indubitablement la technique la plus sûre, la plus fiable. Néanmoins, elle est si intrusive au regard des libertés individuelles et collectives qu'elle est utilisée et centralisée dans des fichiers selon des règles très précises et minutieuses, auxquelles il ne convient pas de contrevenir. Les fichiers d'empreintes génétiques posent problème au regard de la protection des données à caractère personnel ; il convient de garder en mémoire cet aspect dont il sera question plus tard.

Avec le XXI^e^ siècle, des recherches nombreuses sont menées sur les applications biométriques. Les industriels participent volontiers au financement de ces recherches car les nouveaux procédés sont vite utilisés et le retour sur investissement est notable. C'est pourquoi des progrès ont été réalisés pour tous les procédés déjà existants et c'est aussi pourquoi des pistes nombreuses sont explorées : système veineux, lobe de l'oreille, contour des lèvres peuvent notamment être cités. Les moyens biométriques s'insèrent dans la vie sociale et permettent un contrôle collectif (passeports, visas) ou individuels (respect des horaires de travail). Les acteurs principaux sont les états, les

9. Commission des Nations unies pour le droit commercial international, à l'origine de lois-types qui ont servi de références pour l'arbitrage, pour les garanties bancaires, pour les questions juridiques inhérentes au commerce électronique.

sociétés commerciales, mais les organisations internationales sont aussi partie prenante du jeu d'échecs biométrique[10].

La vidéosurveillance existe aussi depuis longtemps, mais elle tend à se généraliser depuis les deux dernières décennies. Elle est apparue dans l'Allemagne nazie, qui, pour tenter de mener à bien ses projets de conquête universelle, recourait à la science sous ses aspects militaires[11] et civils. La vidéosurveillance prit cependant son essor après la Seconde Guerre mondiale. Sa première patrie d'élection fut le Royaume-Uni, à partir des années 1950 et un essor est notable dans les années 1990. Actuellement les caméras, analogiques puis numériques, sont installées un peu partout en Grande-Bretagne, dans les autoroutes, dans les moyens de transport, dans les magasins, etc. Cette mise en œuvre systématique a permis aux chercheurs britanniques de prendre du recul par rapport à l'installation et à la maintenance de ces moyens de surveillance systématiques. Il apparaît que la délinquance et la criminalité ne sont guère affectées par cette généralisation de la vidéosurveillance et pourtant, l'idéologie sécuritaire britannique s'appuie sur la nécessaire lutte contre la délinquance et la criminalité, puis contre le terrorisme, après les attentats, notamment les attentats aveugles du 7 juillet 2005 pour justifier les investissements publics dans ce domaine. La vidéosurveillance a plusieurs domaines de dilection et de prédilection : le réseau routier (la finalité est de lutter contre les infractions au Code de la route et de limiter les accidents, de réduire la mortalité et le handicap) ; les moyens de transports collectifs (la finalité est la protection des voyageurs contre les diverses formes de délinquance) ; les centres commerciaux ; les banques (la finalité est la réduction des vols) ; les établissements ouverts au public, tels les hôpitaux ; les universités (la finalité est la sécurité des visiteurs et des utilisateurs, patients, étudiants). Le financement, au Royaume-Uni, est public ou privé.

La vidéosurveillance s'est étendue dans la plupart des pays développés, voire des pays en cours de développement. Elle s'est accrue considérablement aux Etats-Unis, mais moins vite qu'au Royaume-Uni. En France, la vidéosurveillance n'était mise en œuvre qu'avec parcimonie jusqu'à la fin du XX^{e} siècle ; la première loi importante date du 21 janvier 1995. Dès cette loi, qui demeure essentielle, il apparaît que les films sont des données à caractère personnel, qui doivent donner lieu à une déclaration. L'essor de la vidéosurveillance en France dépend dans un premier temps très largement des municipalités et de leurs édiles. En France, la mise en place de caméras de vidéosurveillance nécessite une demande d'autorisation auprès du préfet, qui travaille à ce sujet en collaboration avec des commissions départementales. A Paris, la demande d'autorisation est effectuée auprès du préfet de police de la ville de Paris. Les

10. HCR, ONU en particulier en Afghanistan.

11. Tentative d'obtenir la bombe atomique, avantage comparatif appréciable.

finalités sont assez proches de celles qui existent au Royaume-Uni et s'appliquent à la sécurité des personnes et des biens. Sont concernés : les abords de bâtiments qui peuvent présenter un risque, le trafic routier afin de prévenir les infractions et les accidents[12], les bâtiments de la Défense nationale, les transports en commun et notamment le métro et les bus, les centres commerciaux. La vidéosurveillance s'intéresse par ailleurs beaucoup aux établissements ouverts au public. En France, toute demande d'autorisation implique le dépôt d'un dossier auprès de la préfecture, avec plan de masse et individualisation de l'emplacement des caméras. Les personnes concernées ont un droit d'accès aux films les concernant, puisque cela correspond, *via* l'identification des images, à des données à caractère personnel. Après usage, les films sont détruits, sauf s'ils constituent des preuves à présenter devant un tribunal.

Le financement en France a d'abord été assez timide, car beaucoup de préfets et de maires ne percevaient pas l'utilité de mettre en place des caméras. C'est donc une volonté politique qui a présidé à l'installation de plus en plus répandue de caméras de vidéosurveillance. En France, un plan d'installations a été décidé sous plusieurs ministres de l'Intérieur successifs et l'accompagnement législatif a été celui de la Loppsi 1, puis de la Loppsi 2.

Les politiques se sont, dans tous les états-nations, appuyés sur un sentiment d'insécurité qui existait à l'état latent chez la plupart des citoyens et a été exploité à l'occasion de la médiatisation des faits divers : crimes, petite délinquance surtout. Les citoyens ont le sentiment, largement fallacieux, d'être protégés par la présence des caméras. Cette dernière dissuaderait les délinquants et les criminels de passer à l'acte. Ce sentiment est erroné ; tout au plus certains délinquants sont-ils parfois amenés à déplacer le terrain de leurs exploits sur d'autres lieux et encore, cette délocalisation est souvent passagère. En France, la terminologie a été modifiée pour entériner ces frayeurs populaires largement exploitées par les médias et les élus. Depuis la loi Loppsi 2 du 14 mars 2011, il n'est plus question de vidéosurveillance, mais de vidéoprotection, qui semble plus correcte et positive.

Cependant, comme la vidéoprotection est un moyen de contrôle, dans la majorité des pays, un recours est prévu en cas de dérives. En France, une commission nationale de la vidéoprotection a été instaurée. Puis, la CNIL s'est vue confier une mission générale de recours afin de protéger les libertés individuelles et collectives protégées par la Convention européenne de sauvegarde des droits de l'homme et des

12. Cependant, aucune corrélation évidente n'existe entre la diminution, depuis une dizaine d'années, de la mortalité sur les routes en France et la mise en œuvre des caméras de vidéosurveillance.

libertés fondamentales[13] du Conseil de l'Europe, la Charte européenne des droits fondamentaux de l'Union européenne[14]. Des plaintes peuvent être déposées auprès de la CNIL si la finalité poursuivie par l'enregistrement n'est pas la sécurité des personnes et des biens. Dans presque tous les états industrialisés, les salariés sont filmés pendant leur journée de travail. L'objectif est d'assurer la sûreté des biens, du matériel, des collaborateurs ; la finalité que serait la surveillance constante des salariés est incompatible avec les textes principaux en matière de libertés[15]. Le consentement même des salariés ne justifie pas la légitimité de l'opération. L'entreprise, l'employeur ne sont pas en droit d'utiliser les caméras à des fins de management, pour améliorer le rendement des travailleurs et assurer une compétitivité accrue à l'entreprise. Il est cependant évident que certaines dérives sont effectives et les plaintes se sont multipliées devant les entités qui sont habilitées à les recevoir et, éventuellement, à les traiter. En France, c'est la CNIL qui reçoit les plaintes. Les mises en demeure rendues publiques sont assez rares mais le nombre de plaintes ne cesse de croître, ce qui tend à laisser penser que certaines personnes, malgré l'influence sur elles de l'idéologie sécuritaire, ne sont pas prêtes à être contrôlées pendant toute leur journée de travail.

Si interceptions et vidéoprotection existent depuis longtemps mais ont vu leur importance progresser dans les rouages du corps social au XXI^e^ siècle, certaines méthodes de contrôle sont apparues au XXI^e^ siècle : il s'agit notamment du scanner à usage corporel et des fichiers génétiques.

Selon Bruno Latour, « Les techniques appartiennent au règne des moyens et la morale au règne des fins, même si, comme Jacques Ellul en a témoigné il y a bien longtemps, certaines techniques finissent par envahir tout l'horizon des fins en se donnant à elles-mêmes leurs propres lois, en devenant autonomes et non plus seulement automatiques »[16]. Les techniques ont envahi l'horizon des fins : c'est le cas de la biométrie notamment, facteur d'identification numérique.

Le scanner corporel, à première vue semble appartenir au règne des moyens mais la question de ses rapports avec le règne des fins reste posée. Il existe deux formes de scanners corporels : le scanner corporel à ondes millimétriques et le scanner corporel qui a recours à la technique de la rétrodiffusion des rayons X. Le plus utilisé est le scanner à ondes millimétriques ; c'est le cas aux Etats-Unis, au Royaume-Uni, aux

13. Article 8 relatif à la vie privée.

14. Articles 7 et 8.

15. Voir rapport de la CNIL sur la cybersurveillance au travail en 2004.

16. Latour Bruno, « La fin des moyens », *Réseaux-Communication-Technologie-Société*, p. 39, vol. 18, n° 100, 2000.

Pays-Bas, en Allemagne, en Italie, en France, au Canada. Les détecteurs à balayage corporel fonctionnent avec des micro-ondes. Les appareils domestiques qui font usage d'ondes millimétriques jouent un rôle éminent dans la plupart des pays occidentaux avec les fours à micro-ondes[17], la téléphonie cellulaire[18], le réseau Wi-Fi[19]. Seule, une partie insignifiante de l'énergie des radiofréquences émise par le scanner est absorbée à la surface du corps, tandis que la majeure partie du rayonnement est réfléchie puis captée par des senseurs afin de produire une image en trois dimensions. Les scanners sont utilisés essentiellement dans les aéroports, malgré le principe de liberté de circulation qui relève à la fois du droit économique, de la liberté des échanges commerciaux et des droits de l'homme[20].

Les scanners corporels ont été installés en grand nombre aux Etats-Unis : 385 scanners, d'un coût élevé, étaient déjà installés en 2010 dans plus de 60 aéroports. Ce sont les Etats-Unis qui ont initié la mise en place des scanners corporels dans la plupart des pays occidentaux, dans le cadre des aéroports, avec pour objectif la sécurisation des déplacements aériens. Certains états résistent à la pression américaine mais les plus proches alliés des Etats-Unis suivent leur exemple.

Dans le domaine médical, des études ont été menées. Elles n'ont pas abouti à des conclusions définitives mais nourrissent des craintes afférentes au cancer. Le principe de précaution doit-il être appliqué ? Pour les Etats-Unis, la réponse est négative.

De nombreux américains considèrent aussi que le scanner corporel porte atteinte à la vie privée : le scanner corporel révèle, ne serait-ce qu'aux agents de la TSA[21], l'intimité des personnes contrôlées et un grand nombre de citoyens redoutent que leurs photographies se retrouvent sur Internet, y compris sur les réseaux sociaux. Un mouvement de boycott du scanner corporel a été lancé la veille du Thanksgiving Day 2010. Le Thanksgiving a été choisi parce que cela correspond à un jour où les américains voyagent beaucoup et empruntent les aéroports. Le droit à l'intimité et à la vie privée, qui serait mis à mal par le scanner corporel, a été relayé par de multiples associations de droits de l'homme. Ainsi, l'Epic[22] a déposé une plainte pour suspendre le déploiement des scanners corporels dans les aéroports américains

17. 24 à 30 GHz.
18. 0,9 à 2,1 GHz.
19. 2,45 GHz.
20. Article 2.1 du Pacte international des droits civils, 1966, « Liberté d'aller et de venir ».
21. Transportation Security Administration.
22. Electronic Privacy Information Center.

car ils seraient « illégaux, invasifs et inefficaces »[23] ; cette plainte n'a pas abouti. Les autorités américaines, dans un contexte où la géopolitique n'est pas absente, pressent les gouvernements européens de renforcer la sécurité dans les transports aériens et d'introduire le scanner corporel.

Au niveau de l'Union européenne, le Parlement européen a demandé, dans une résolution du 23 octobre 2008, l'établissement d'un rapport ayant pour objectif l'évaluation des scanners corporels sur les plans de la santé et du respect des droits fondamentaux. La Commission est invitée à consulter le contrôleur européen de la protection des données, l'Agence des droits fondamentaux. Un débat est organisé en janvier 2010 par la Commission des libertés civiles à l'occasion d'une réunion avec le coordinateur de la politique antiterroriste[24]. La politique d'installation de scanners corporels était censée trouver sa place dans une optique élargie où il est fait mention de partage des données entre l'Union européenne et les Etats-Unis. Les députés de la Commission des libertés civiles sont d'avis qu'avant de recourir aux scanners corporels, il convient de continuer à évaluer le système d'information Schengen et le système d'information sur les visas pour déterminer si ces systèmes sont efficaces et conformes aux principes régissant la protection des données à caractère personnel. Un débat intervient ensuite devant la Commission des transports en janvier 2010. Une ambivalence apparaît en matière de vie privée. Les uns, comme la Britannique Jacqueline Foster, sont favorables au profilage et à l'échange d'informations pour améliorer la fiabilité de la technologie. D'autres, au contraire, sont attachés avant tout à la préservation de la vie privée. Cela implique, au minimum, que les images ne soient pas cédées aux organes de presse. Par ailleurs, il est indispensable que les images, qui sont des identifiants, soient détruites immédiatement après utilisation. Certes, les contrôleurs aéroportuaires ne sont pas autorisés à enregistrer les images mises en cause, mais il suffit d'un téléphone portable pour réaliser un cliché ; une dérive peut amener la reproduction du corps d'un adulte ou d'un enfant sur support numérique. Le 15 juin 2010, la Commission européenne présente un rapport d'évaluation sur le scanner corporel. La finalité du scanner est la détection d'objets et non l'identification des personnes physiques. En conséquence, aucune image réalisée par les scanners ne doit être conservée. Dans le cas contraire, *via* la constitution de fichiers d'images des corps des passagers aériens, il y aurait un détournement de finalité, en violation de la directive 95/46, de la résolution de l'Assemblée générale de l'ONU du 14 décembre 1990. Par ailleurs, la personne ne doit pas pouvoir être identifiée ; pour ce faire, il convient de recourir au floutage du visage. L'identification ne sera envisagée que si des objets dangereux sont découverts. Afin de garantir l'anonymat des personnes scannées, les contrôleurs travaillent en binôme : l'un d'eux

23. Epic.org/privacy/airtravel/backscatter.

24. A cette époque, De Kerkhove G.

a pour mission de faire entrer le voyageur dans le scanner ; le deuxième examine l'écran de visualisation et procède au contrôle, mais sans contact direct avec le passager objet du contrôle.

Le 24 mai 2011, la Commission des transports et du tourisme au Parlement européen a voté le rapport élaboré par le conservateur espagnol Luis De Grandes Pascual[25] à une très large majorité. Ce rapport est dédié à la sécurité aérienne et notamment au recours au scanner corporel dans les aéroports.

L'utilisation des scanners corporels serait un facteur de renforcement de la sûreté aérienne. Cette machine a été expérimentée au Royaume-Uni, aux Pays-Bas, en Finlande, en France, en Italie[26]. Depuis 2008, année où le Parlement européen avait fait mention de son opposition à l'introduction du scanner corporel, la situation a grandement évolué : « Quatre ans plus tard (…) nous considérons que ces appareils peuvent offrir une valeur ajoutée en termes de sécurité sans risque pour la santé des passagers ou doute sur le respect de leurs droits fondamentaux ». Le rapport demande aux états membres « de faire usage de la technologie qui soit la moins nocive possible[27] pour la santé des personnes » et interdit les scanners qui font appel aux radiations ionisantes, c'est-à-dire les scanners utilisant des rayons X, afin de prendre en compte la fragilité des personnes vulnérables. Les personnes considérées comme vulnérables sont les femmes enceintes, les personnes âgées, les enfants, les malades.

La vie privée se doit d'être respectée. Le refus d'être soumis au scanner corporel a pour corollaire l'obligation de se soumettre à une méthode d'inspection de substitution, qui garantit une efficacité équivalente, comme la fouille corporelle. Le refus « ne doit pas jeter une quelconque suspicion sur le passager ». Luis De Grandes Pascual reconnaît pourtant que l'alternative, le recours à la fouille corporelle manuelle, comme cela est apparu évident aux Etats-Unis, pouvait compliquer et retarder l'embarquement des passagers qui refusent l'utilisation sur leurs personnes de scanners corporels. Lorsque les personnes physiques acceptent d'être soumises au contrôle du scanner corporel à ondes millimétriques, une sélection aléatoire est appliquée et les passagers ne doivent pas être sélectionnés sur la base de critères discriminatoires : « Toute forme de profilage fondée notamment sur le sexe, la race, la couleur, l'origine ethnique ou nationale, les caractéristiques génétiques, la langue,

25. PPE.

26. En Italie, des scanners corporels ont été déployés dans plusieurs aéroports du pays, mais, au bout de quelques mois, les scanners ont été retirés puisqu'ils ont été considérés comme inutiles et incompatibles avec le respect de la vie privée, comme l'a fait remarquer Vito Riggio, président de l'ENAC, l'Ente Nazionale per l'Aviazione Civile.

27. Le rapport ne prétend pas à une innocuité absolue.

la religion ou les convictions est inacceptable ». Cela est parfaitement compatible avec la directive n° 95/46 et avec l'actuel projet de règlement. L'image ne doit pas être un élément d'identification absolue. Il convient de prendre en compte la dignité humaine et l'intimité. Seules les silhouettes du type *stick figure*[28] doivent être utilisées. Aucune image du corps humain ne doit être prise, stockée, enregistrée. Les images, selon les eurodéputés, sont détruites tout de suite après le passage du contrôle de sécurité. Surtout « La technique utilisée ne doit pas permettre de conserver ou de sauvegarder des données ».

L'eurodéputée Sylvie Guillaume fait remarquer sur son blog qu'un progrès important a été réalisé depuis 2008, que les critiques afférentes à la santé et à la vie privée n'ont pas été ignorées. Néanmoins elle demeure sceptique sur l'utilité des scanners corporels à ondes millimétriques. D'autres techniques de contrôle, *a priori* moins intrusives, sont en mesure de procéder à des contrôles de type identique dans les aéroports. Le scanner corporel n'a pas démontré sa plus grande efficacité. Aucune étude sérieuse n'a fait la preuve de sa valeur ajoutée dans la lutte contre le terrorisme ; or, c'est la principale justification énoncée lors de son installation. Le conservateur allemand Markus Ferber est plus réservé que Sylvie Guillaume : « Les scanners corporels portent atteinte à la sphère privée, sans gain évident en matière de sécurité ». Sylvie Guillaume insiste sur le lien entre la technique et l'industriel : plusieurs entreprises proposent sur le marché des scanners corporels coûteux mais qui sont la source d'importants retours sur investissements pour les constructeurs. Ces derniers constituent un lobby afférent au contrôle sur les aéroports et savent se faire entendre. Ils sont en mesure de faire évoluer leur machine, leur produit pour qu'ils soient compatibles avec les exigences juridiques en matière de protection de la vie privée et des données à caractère personnel.

Les eurodéputés sollicitent la mise en place d'une collaboration au niveau de l'Union européenne dans le domaine de la sûreté aérienne. Cela implique la reconnaissance mutuelle des mesures envisagées et un contrôle de sécurité unique pour les passagers, les bagages et le fret dans les aéroports de l'Union européenne. Il s'agit en fait d'une coordination entre les états de l'Union européenne. Des discussions sont toujours menées entre les Etats-Unis, initiateurs de l'introduction du scanner corporel et l'Union européenne, qui est sans doute plus exigeante que les Etats-Unis en matière de santé et de vie privée.

Le Parlement européen adopte, le 6 juillet 2011, une résolution pour encadrer l'utilisation du scanner corporel en s'inspirant du rapport Pascual. La résolution précède la décision de la Commission pouvant autoriser les scanners corporels dans

28. « Bonhomme-allumette ».

les aéroports. Le Parlement est en mesure d'annuler la décision dans un délai de trois mois. Les députés européens souhaitaient que les Gouvernements européens se dotent de la technologie convenable avant fin avril 2013, date à laquelle l'interdiction de transporter des liquides par voie aérienne devait être levée. C'est pourquoi la Commission, qui entendait faire respecter le délai de 2013, a annoncé la mise en place d'un groupe de travail comprenant des représentants des états et des responsables de l'industrie et de l'aviation.

La Commission a en effet fait savoir dans sa communication que les passagers ne seront pas choisis « uniquement » sur des critères tels que le sexe, la race, la couleur de peau, l'origine sociale ou ethnique, la religion ou les convictions[29]. Or, il s'agit de données sensibles et la directive 95/46 indique que les données à caractère personnel qui entrent dans cette catégorie ne doivent pas être conservées et *a fortiori* utilisées, sauf exceptions ou consentement préalable. Cela constitue donc clairement une discrimination à laquelle seraient confrontées les personnes qui feraient l'objet d'un contrôle par scanner à ondes millimétriques. Le risque de profilage, racial ou autre, semble possible. Il convient de déterminer si le terme « uniquement » sera maintenu.

La Commission européenne a décidé qu'« afin de ne pas risquer de compromettre la santé des citoyens, seuls les scanners corporels, n'utilisant pas la technologie des rayons X sont autorisés pour le contrôle des passagers dans les aéroports de l'Union européenne. Toutes les autres technologies, telles que celles utilisées pour les téléphones mobiles et autres peuvent être utilisés à condition qu'elles soient conformes aux normes de sécurité de l'Union européenne ». Cela a déclenché des réactions négatives au Royaume-Uni dans deux aéroports recourant à des scanners à rayon X à Manchester et à Heathrow. L'aéroport de Manchester a publié la déclaration suivante : « Des tests approfondis par l'Agence britannique de protection de la santé et les autorités sanitaires américaines ont déjà confirmé que les scanners corporels posent un risque négligeable pour la santé humaine. Il est irresponsable de laisser entendre que, parce que l'Europe n'a pas encore terminé son étude santé, nos passagers devraient être concernés. La législation européenne a approuvé cette semaine la technologie à ondes millimétriques, une autre forme de technologie de scanner corporel, pour une utilisation permanente dans les aéroports (…) Etant donné que toutes les autorités compétentes autorisent l'utilisation des scanners corporels à rayon X, l'usage va se poursuivre ». A Heathrow, la situation était différente car si l'aéroport avait utilisé précédemment des scanners à rayons X dans le cadre d'une évaluation des différentes technologies de scanners corporels, une fois l'évaluation menée à son terme, l'aéroport a eu exclusivement recours à des

29. Communication de la Commission au Parlement européen relative à l'utilisation de scanners de sûreté dans les aéroports de l'Union européenne, COM (2010) 311, §50.

scanners corporels à ondes millimétriques. En France, Aéroports de Paris a pu se féliciter d'avoir anticipé sur le bon choix, car les expérimentations menées à Paris utilisaient le scanner à ondes millimétriques. C'est la Loppsi 2 qui légifère[30] en France en matière de scanners corporels. Elle suit les recommandations du G29[31] et de la CNIL.

La visualisation des images est restreinte à un personnel compétent et habilité dans des locaux qui ne sont pas ouverts au public. Les personnes qui procèdent au contrôle appartiennent au même genre que le passager ou la passagère. Ces dispositions avaient été antérieurement introduites pour les palpations de sécurité. La conservation des images est limitée à la durée indispensable au contrôle. La visualisation des images s'effectue dans des locaux interdits au public et est circonscrite aux personnes habilitées. Surtout, les fouilles et visites ne peuvent être réalisées qu'avec le consentement de la personne physique contrôlée. En cas de refus, la personne est soumise à un autre dispositif de contrôle, en général, la palpation manuelle, qui n'est d'ailleurs pas sans poser de problème quant au respect de l'intimité et de la dignité. Le scanner corporel ne peut pas être utilisé sans un consentement libre et éclairé. L'analyse des images visualisées est effectuée par des opérateurs qui ne connaissent pas l'identité des personnes physiques et qui ne sont pas en mesure de visualiser simultanément la personne physique et son image produite par le scanner corporel.

Les fichiers génétiques, qui relèvent de la biométrie mais sont utilisés par la police, utilisent des technologies efficaces qui sont apparues et ont été utilisées à la fin du XX^e^ siècle et au début du XXI^e^ siècle.

Les empreintes génétiques sont assimilées à des données biométriques. La biométrie, selon le dictionnaire[32] est « la science qui étudie, à l'aide des mathématiques (statistiques, probabilités) les variations biologiques à l'intérieur d'un groupe déterminé ». Cette définition s'applique parfaitement à l'ADN. De plus, les autorités de régulation, telles la CAI[33] au Québec ou la CNIL en France ajoutent aux distinctions mentionnées plus haut entre biométrie morphologique et biométrie comportementale, l'analyse des empreintes génétiques. Les fichiers génétiques britannique et français ont tout de suite posé problème au regard de l'équilibre entre sécurité-ordre public et préservation de la vie privée.

30. Loi du 14 mars 2011.

31. Regroupement, dans le cadre de la directive 95/46, des représentants des autorités de régulation, en référence à l'article 29 de la directive.

32. *Petit Robert*, 2014.

33. Commission d'accès à l'information.

Le 4 décembre 2008, la grande chambre de la Cour européenne des droits de l'homme a condamné le Royaume-Uni pour violation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[34].

A l'origine de l'affaire, doivent être mentionnées deux personnes, S.[35] et Michael Marper[36], citoyens du Royaume-Uni.

Le premier requérant fut appréhendé le 19 janvier 2001 et inculpé de tentative de vol avec violences ; il avait alors onze ans, était mineur. La police préleva ses empreintes digitales et des échantillons d'ADN. Il fut acquitté le 14 juin 2001. Le second requérant fut appréhendé le 13 mars 2001 et inculpé de harcèlement à l'égard de sa compagne. La police préleva ses empreintes digitales et des échantillons d'ADN. La compagne de Michael Marper se réconcilia avec lui, retira sa plainte ; le 14 juin 2001, l'affaire fut classée sans suite.

Les deux requérants souhaitaient que les empreintes digitales et les échantillons d'ADN fussent détruits et se heurtèrent à un refus de la police. Ils saisissent la justice. Le 22 mars 2002, le tribunal administratif[37] les déboute[38]. Le 12 septembre 2002, la Cour d'appel confirme la décision du tribunal administratif par une majorité de deux voix contre une. Le 22 juillet 2004, la Chambre des lords déboute à son tour les requérants. L'arrêt est rendu par Lord Steyn, au nom de la majorité.

Ayant épuisé les voies de recours interne, S. et Marper introduisent une requête individuelle devant la CEDH. Ils se plaignent de la conservation de leurs empreintes digitales, échantillons cellulaires et produits génétiques. Ils s'appuient sur les articles 8 et 14[39] de la Convention EDH. En particulier, ils estiment qu'il y a eu violation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, consacré à la vie privée. La Cour recherche tout d'abord si la conservation par les autorités des empreintes digitales, échantillons cellulaires et profils ADN des requérants peut constituer une ingérence dans leur vie privée. La CEDH estime que le caractère général et indifférencié de la conservation des empreintes digitales, échantillons biologiques et profils ADN de personnes soupçonnées d'avoir commis des infractions, mais non condamnées, ne correspond pas à « un juste équilibre » entre les

34. CEDH, 4 décembre 2008, numéros 30562/04 et 30566/04, Set Marper c. Royaume-Uni.
35. Le premier requérant.
36. Le deuxième requérant.
37. Lord Justice Rose et le juge Leveson.
38. EWHC 478.
39. Discrimination.

intérêts publics et les intérêts privés : il s'agit d'une atteinte disproportionnée au droit des requérants, au respect de la vie privée et n'est pas nécessaire dans une société démocratique. Il y a bien violation de l'article 8 de la Convention et il n'y a pas lieu d'examiner séparément le grief tiré de l'article 14 de la Convention. Le Royaume-Uni doit verser aux requérants 42 000 euros pour frais et dépens.

Le Gouvernement britannique fait valoir que le risque d'intervention dans la vie privée est limité par la loi et les procédés technologiques d'extraction[40]. La CEDH mentionne qu'une distinction a déjà été établie entre la conservation des empreintes digitales, celle des échantillons cellulaires et les profils d'ADN. La question du respect de la vie privée doit être analysée séparément pour la conservation des échantillons cellulaires, les profils ADN et pour la conservation des empreintes digitales. Précédemment[41], la CEDH a estimé que, dans le cas des échantillons cellulaires, la conservation systématique de pareils éléments était trop intrusive. « De surcroît, les échantillons renferment un Code génétique unique qui revêt une grande importance tant pour la personne concernée que pour sa famille ». La Cour mentionne que le concept de vie privée est une notion large. « (…) Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 ». Une ingérence est considérée comme indispensable pour atteindre un but légitime dans une société démocratique si elle est proportionnée au dit but légitime et si les motifs invoqués par les autorités nationales semblent « pertinents et suffisants »[42]. Une marge d'appréciation est laissée aux autorités nationales. Mais les empreintes digitales, les profils ADN, les échantillons cellulaires « constituent toutes des données à caractère personnel au sens de la Convention (…) car elles se rapportent à des individus identifiés ou identifiables ». Les différentes données biométriques sont analysées, en particulier les profils ADN qui « fournissent un moyen de découvrir les relations génétiques (et ethniques) pouvant exister entre des individus ce qui suffit en soi pour conclure que leur conservation constitue une atteinte au droit à la vie privée de ces individus ». Un raisonnement identique s'applique aux empreintes digitales numérisées. La CEDH reconnaît que la lutte contre le crime est un but légitime. Dans les moyens qui sont déployés pour combattre le crime, le Conseil de l'Europe a reconnu que les techniques d'analyse de l'ADN présentaient certains avantages. La question qui se pose est donc la suivante : la conservation des empreintes digitales et données ADN de S. et de Michael Marper, soupçonnés d'avoir commis des infractions mais non condamnés se justifie-t-elle sous l'angle de l'article 8, paragraphe 2 de la Convention ? LA CEDH affirme que l'Angleterre, le Pays de Galles et l'Irlande du

40. « Une personne ne serait identifiée que dans le cas d'une concordance de son profil avec l'un de ces éléments et dans la mesure de cette concordance ».

41. Affaire Van der Velden, 7 décembre 2006.

42. CEDH, 18 janvier 2001, n° 24876, Coster c. Royaume-Uni.

Nord sont « les seuls ordres juridiques au sein du Conseil de l'Europe à autoriser la conservation illimitée des empreintes digitales et des échantillons et profils d'ADN de toute personne, quel que soit son âge, soupçonnée d'avoir commis une infraction emportant inscription dans les fichiers de la police ». D'autres états ont décidé de fixer des limites à la conservation et à l'utilisation de ces données afin de parvenir à un bon équilibre entre l'ordre public et la préservation de la vie privée. Le Royaume-Uni insiste sur l'efficacité de ces données en cas d'infraction. Ni les statistiques ni les exemples fournis ne permettent d'établir qu'il serait impossible d'identifier et de poursuivre des auteurs de crimes et de délits sans la conservation permanente des empreintes digitales et données ADN. Au demeurant, la conservation des données afférentes à des personnes non condamnées est particulièrement préjudiciable lorsque les personnes en cause sont mineures. La CEDH a mis l'accent sur la sauvegarde de la vie privée des mineurs dans les procédures pénales[43]. Au Royaume-Uni même, le Nuffield Council avait fait connaître ses réserves quant aux conséquences avérées pour les jeunes d'une conservation illimitée de leurs échantillons et profils ADN : les mineurs et les membres des minorités ethniques qui n'ont pas été reconnus coupables d'infraction sont surreprésentés dans la base de données.

La CEDH retient par ailleurs une atteinte disproportionnée au droit des requérants. Le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes physiques soupçonnées d'avoir commis des infractions mais non condamnées ne correspond pas à un juste équilibre entre les intérêts publics des autorités nationales et les intérêts privés en jeu ; en outre, le Royaume-Uni a outrepassé toute marge d'appréciation en la matière. La CEDH n'examine pas les critiques formulées par les demandeurs à l'encontre de certains points du régime de conservation des données, tels l'accès, trop large selon eux, à ces données et l'insuffisance de la protection offerte contre les usages impropres ou abusifs. « Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique ».

Parmi ces états démocratiques, une comparaison peut être établie entre la Grande-Bretagne et la France.

En Grande-Bretagne, le fichier des empreintes génétiques a été créé en 1995, mais seulement pour des affaires criminelles. En France, le FNAEG (fichier national automatisé des empreintes génétiques) a été institué par la loi Guigou du 18 juin

43. CEDH, 16 décembre 1999, n° 247224/94, T. c. Royaume-Uni, § 75 et 85.

1998[44] uniquement pour recueillir les empreintes génétiques des personnes impliquées dans les infractions à caractère sexuel.

Au XXIe siècle, les infractions pour lesquelles des empreintes génétiques sont prélevées sont de plus en plus fréquentes. Au Royaume-Uni, la loi a évolué en 2001, puis en 2004. Depuis 2004, les ADN des personnes mises en cause de quelque façon que ce soit dans un délit, dont la police peut garder trace en Angleterre, au Pays de Galles et en Irlande du Nord sont stockés pour toujours.

En France, l'article 706-55 du Code de procédure pénale précise dans quel cas le prélèvement et la conservation des empreintes génétiques est possible : pour les personnes condamnées pour l'une des infractions mentionnées à l'article 706-55 du Code de procédure pénale, pour les personnes à l'encontre desquelles peuvent être retenus des indices graves ou concordants rendant possible la commission d'une infraction, pour les personnes à l'encontre desquelles il existe des raisons de penser qu'elles ont commis un crime ou un délit. En outre, selon l'article R. 53-10 du Code de procédure pénale, il est également possible de procéder à des prélèvements dans les cas suivants : des traces biologiques, issues de personnes inconnues sont recueillies dans le cadre d'une enquête préliminaire, d'une enquête pour crime ou délit flagrant ou d'une instruction préparatoire ; des échantillons biologiques sont prélevés sur des cadavres non identifiés et des traces biologiques sont issues de personnes inconnues ; ils sont recueillis dans le contexte d'une enquête ou d'une instruction pour recherche des causes du décès ou pour recherche des causes d'une disparition non élucidée ; des échantillons biologiques sont issus ou peuvent être issus d'une personne disparue et recueillis dans le cadre d'une enquête ou d'une instruction pour recherche des causes d'une disparition non élucidée ; des échantillons biologiques sont prélevés, avec leur consentement, sur les ascendants ou les descendants d'une personne disparue, dans le contexte d'une enquête ou d'une instruction pour recherche des causes d'une disparition non élucidée.

Les bases de données témoignent de l'importance du phénomène. La Grande-Bretagne possède la base de données la plus importante, avec 4,3 millions d'empreintes génétiques en 2008, dont 850 000 au minimum appartiennent à des témoins, des victimes ou des personnes que la justice a décidé de ne pas poursuivre ou qui ont été acquittées.

Les empreintes génétiques stockées sont donc particulièrement intrusives et les bases de données tendent à s'élargir de plus en plus. Il en est de même pour les fichiers de police centralisés.

---

44. Article 28.

Les technologies sont donc de plus en plus fréquemment utilisées pour contrôler la population.

Dans quelle mesure l'apparition des technologies numériques a-t-elle amené les juristes et les politiques à recourir à ces moyens pour surveiller non seulement les ennemis de la démocratie, mais une grande partie de la population ?

Les droits de l'homme, idéologie qui n'a pas cessé de se développer, sont-ils remis en cause insidieusement par l'utilisation des technologies ?

L'objet de cet ouvrage est de tenter de déterminer si l'équilibre entre ordre public et préservation des droits fondamentaux est encore à l'ordre du jour, alors que le curseur penche délibérément du côté de la sécurité. Il ne s'agit pas d'une étude théorique, mais empirique. Il est fait appel au droit et, dans une moindre mesure, aux sciences politiques.

L'aspect diachronique est mis en exergue : dans un premier temps, il sera fait état de l'histoire enchantée et chimérique du temps où ordre public et respect de la vie privée souhaitaient se concilier.

Dans un deuxième temps, il sera question du temps qui coïncide avec la survenance du XXI^{e} siècle, où la sécurité, avec ses aspects économiques, financiers, juridiques semble l'emporter sur l'utopie des droits de l'homme.

Enfin, après la crise économique de 2008, survient le temps actuel où le tout sécuritaire entre en dichotomie avec des jurisprudences qui renouent avec les textes fondamentaux relatifs aux droits de l'homme.