IMPACTS DE L'UTILISATION DES TECHNOLOGIES DE SURVEILLANCE BIOMÉTRIQUES ET COMPORTEMENTALES DE MASSE SUR LES DROITS HUMAINS ET L'ÉTAT DE DROIT

Traduction française du résumé analytique et de la conclusion du rapport :

IMPACTS OF THE USE OF BIOMETRIC AND BEHAVIOURAL MASS SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS AND THE RULE OF LAW[1]

Rapport commandé par les Verts/ALE au Parlement européen.

Auteurs : Estelle De Marco et Aeris
Contributrices : Célie Zamora et Valentina Pavel
Relecture linguistique de la version anglaise : Mireille Renaud-Mallet

Traduction française[2] : Estelle De Marco, mai 2025.

[1] Estelle De Marco *et al.*, Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the Rule of law, février 2022, https://extranet.greens-efa-service.eu/public/media/file/1/7487.

[2] Les références associées au texte traduit se trouvent dans la version anglaise du rapport, à partir de son introduction p. 21.

1. RÉSUMÉ ANALYTIQUE

SECTION 2 : INTRODUCTION

Depuis plusieurs siècles, citoyens et résidents se posent la question des limites que doit connaître le pouvoir de l'État en matière de restriction de leurs libertés et de leur libre arbitre. Chaque fois que ces limites ont paru avoir été dépassées, dans l'histoire, parlementaires et société civile se sont soulevés. Au 18ème siècle, cette opposition était dirigée contre les passeports et l'enregistrement, dans des fichiers, de certaines catégories de personnes comme celles suspectées d'avoir commis une infraction pénale ou les opposants politiques. À la fin du 19ème siècle, l'opinion publique s'est opposée à la collecte par l'État de photographies, considérées comme une menace pour la liberté des « gens honnêtes ». Cette dernière notion paraissait exprimer la peur d'être le sujet d'une classification arbitraire, basée sur des critères obscurs, puis à une privation de liberté contestable, décidée sur la seule base de cette classification.

A partir de la première guerre mondiale, certains gouvernements réussirent à imposer des documents d'identité à tous leurs résidents puis nationaux, des processus permettant en outre, dans certains pays, d'identifier des minorités considérées indésirables. Les cartes d'identité survécurent aux guerres en France, en Italie et en Allemagne, tandis qu'elles furent abolies au Royaume-Uni.

L'opposition aux évènements qui s'étaient produits pendant les guerres conduisit à l'adoption, en 1950, de la Convention européenne des droits de l'Homme (CEDH). L'objet de la Convention était, et reste, de prévenir le retour du totalitarisme, via un mécanisme empêchant les États de favoriser l'ordre et la sécurité au détriment des libertés. Schématiquement, la CEDH impose, au minimum, que toute restriction de liberté fondamentale soit prévue par la loi, qu'elle ait un objet déterminé et légitime (devant correspondre à un besoin démontré) et qu'elle soit tant efficace que réduite au minimum nécessaire pour atteindre cet objectif. Ces principes, aussi appelés « exigences de nécessité et de proportionnalité », ont fait l'objet de transpositions spécifiques dans des lois dédiées à la protection des données personnelles, à partir des années 1970, afin de tenir compte de la numérisation croissante de la société.

À partir de 1985, le développement de la biométrie et de la reconnaissance faciale, de même que leur utilisation croissante par les autorités publiques et le secteur privé, ont alimenté de nouvelles inquiétudes. Les autorités publiques justifient la mise en œuvre et l'accélération du développement de ces technologies comme étant un besoin qui se trouve hors de discussion dans son principe, afin de lutter contre le terrorisme et d'assurer la sécurité. Pourtant et jusqu'à présent, ces autorités ont échoué à apporter des preuves d'efficacité et de valeur ajoutée, alors que la biométrie est hautement intime et identifiante. Par conséquent, la société civile et des politiciens appellent à mettre un terme à cette culture de l'identification et du contrôle, qui est largement considérée comme une menace pour la démocratie et l'État de droit.

Dans ce contexte, la présente étude a pour objet de poser les termes du débat de la manière la plus objective possible, afin d'identifier si les droits de l'Homme et l'État de droit sont menacés par l'utilisation de ces technologies, en se concentrant sur les pratiques des autorités publiques. Cette évaluation se base sur une analyse d'impact sur la vie privé (AIVP) des technologies biométriques et comportementales permettant la surveillance de masse, comprises comme les technologies qui incluent l'utilisation d'identifiants biométriques et qui peuvent permettre une surveillance de masse, même si elles ne sont pas mises en œuvre dans cet objectif particulier.

SECTION 3 : CONTOURS ET CONTEXTE DE L'USAGE DES TECHNOLOGIES DE SURVEILLANCE

Les politiques de gestion des frontières de l'Union européenne (UE) ont imposé successivement la mise en œuvre de biométrie dans les visas, les passeports et les cartes d'identité. Parallèlement, l'objectif de renforcer la gestion des frontières a été étendu à la préservation de la sécurité intérieure des États membres, à la prévention, détection et recherche des auteurs d'infractions terroristes et d'autres infractions graves, et, concernant certaines bases de données, à la coopération policière et judiciaire. À l'heure actuelle, les systèmes d'information qui accompagnent ces politiques, gérés par eu-LISA, rassemblent plus de 53 millions de données biométriques. Ces systèmes sont le VIS, les SIS I et II, ainsi que les systèmes Eurodac, ECRIS, ETIAS et Entrée/Sortie (EES). En outre, ces systèmes utilisent un système automatisé d'identification des empreintes digitales (AFIS), dont il est attendu qu'il inclue à terme la reconnaissance faciale parmi ses principaux composants.

Les États membres de l'UE ont par ailleurs recours de manière croissante à la vidéo-surveillance, qui inclut progressivement des technologies de reconnaissance faciale et comportementale. En outre, les secteurs publics et privés proposent de plus en plus souvent des fonctions d'authentification basées sur de la reconnaissance biométrique. Le secteur privé et le secteur académique ont également tous deux recours à des techniques de surveillance basées sur des critères biométriques ou comportementaux.

L'Union européenne joue un rôle central dans le développement et l'utilisation des technologies biométriques, cherchant à favoriser la convergence technique des systèmes européens qui contiennent des données biométriques. Cette politique de l'UE s'étend aux Balkans occidentaux. Cette approche est parfois présentée comme étant le résultat d'une pression, de la part des Etats-Unis d'Amérique (USA), pour que le recours à la biométrie devienne un objectif prioritaire dans la lutte contre le terrorisme. Pourtant, des auteurs montrent qu'en réalité, l'Union européenne a fait des choix qui dépassent largement les demandes américaines et qui servent plutôt une politique intérieure propre à l'Union, visant à développer un registre d'empreintes digitales et d'images faciales de ses citoyens et résidents.

L'enregistrement d'identifiants biométriques est mis en œuvre dans un contexte où l'Union européenne et les gouvernements tendent à court-circuiter les débats publics et les opinions contraires de parlementaires et d'autorités de protection des données personnelles. Dans le même temps, et au-delà des engagements de pure forme à respecter les droits fondamentaux, les risques posés par ces technologies ne sont, la plupart du temps, pas sérieusement évalués. Cette constatation pose la question d'un affaiblissement intentionnel des parlements et, plus généralement, des contre-pouvoirs démocratiques. En outre, nous observons une forte tendance, de la part des représentants de l'Union européenne et des États membres, à forcer l'"*acceptabilité*" de l'identification et de la reconnaissance biométriques, à travers la création d' « *un climat artificiel de peur »* (Guillaume Gormand), combiné à une communication publique qui présente la surveillance biométrique sous un jour favorable. En effet, elle est montrée comme une promesse de sécurité, la sécurité étant affirmée comme un besoin naturel indiscutable dans son principe et inhérent aux libertés, lorsqu'il n'est pas considéré comme prépondérant. Cette approche constitue un mépris des principes fondamentaux qui fondent le système juridique européen, dans lequel la sécurité est, inversement, une exception à la liberté, sujette à de strictes conditions.

Les citoyens, trompés concernant l'efficacité et les objectifs des technologies biométriques, sont par conséquent privés d'un vrai débat sur ces questions. Pourtant, un tel débat est de la plus grande

importance. En effet, les problèmes de sécurité qui affectent des données intimes qui ne peuvent pas être révoquées, de même que la question de savoir si la sécurité apportée par la surveillance notamment biométrique est réelle, vis-à-vis de la menace terroriste, sont aussi importants que les défis qui se posent en termes de choix de modèle de société, face à celui qui est actuellement suivi.

Sans égard à ces considérations, l'Union européenne soutient l'innovation en finançant différents projets de recherche qui ont pour but d'améliorer l'efficacité de l'identification biométrique ou comportementale, cette recherche ayant été critiquée pour son absence d'éthique. Ce reproche vient en supplément d'allégations concernant le soutien de l'Union européenne à la mise en œuvre de technologies de surveillance dans des pays ayant un faible bilan sur le terrain de la protection des droits de l'Homme, hors de toute étude d'impact.

Dans ce contexte, un nombre significatif d'organisations et d'institutions appellent à une interdiction de la surveillance biométrique, et en premier lieu de la reconnaissance faciale dans les lieux accessibles au public. Ces acteurs incluent l'Organisation des Nations unies, le Parlement européen, le Comité européen de la protection des données (CEPD/EDPB) et le Contrôleur européen de la protection des données (CEDP/EDPS), ainsi que plus de 170 organisations non gouvernementales (ONG).

SECTION 4 : LA LÉGISLATION RÉGLEMENTANT LA SURVEILLANCE

Sous-section 4.1 : Exigences de la CEDH et de la CDFUE

Les excès de l'histoire ont montré l'inaptitude des États à assurer la protection des droits de l'Homme en l'absence de contre-pouvoirs, certainement car l'une des principales caractéristiques inhérentes à tout État est de favoriser l'ordre par rapport aux libertés. En conséquence, la Convention européenne des droits de l'Homme (CEDH) a été signée le 4 novembre 1950 afin d'établir des obligations objectives, pour les États, à l'égard des individus en matière de protection des droits de l'Homme, ainsi que des mécanismes de contrôle destinés à garantir l'exercice de ces droits (les droits de l'Homme étant appelés « droits fondamentaux » lorsqu'ils sont protégés par un texte juridique européen ou international). De nos jours, la CEDH est en vigueur dans les 47 États membres du Conseil de l'Europe, incluant tous les États membres de l'Union européenne.

Il est très important de souligner que le respect de la dynamique de protection des droits fondamentaux consacrée dans la CEDH est la condition du maintien de la démocratie libérale, comprise comme une forme de gouvernement dans laquelle les « *libertés sont bien protégées et dans laquelle il existe des sphères autonomes de société civile et de vie privée, isolées du contrôle de l'État* » (Larry Diamond). En effet, la conception de cette dynamique s'est inspirée des travaux de grands penseurs tels que Beccaria et Tocqueville, qui ont regardé l'histoire avec lucidité et ont averti des dangers qu'il y a à sortir d'un système dans lequel le gouvernement est empêché de donner la priorité à la sécurité au détriment de la liberté. En conséquence, le système juridique est conçu de manière à ce que la liberté et la sécurité ne puisse pas s'opposer.

La dynamique de protection des droits fondamentaux, consacrée dans la CEDH, comprend quatre volets.

- Premièrement, les limitations de libertés doivent être prévues par une loi claire qui assure la prévisibilité.
- Deuxièmement, les limitations de libertés doivent avoir un objectif légitime.

- Troisièmement, les limitations de libertés doivent être efficaces dans la poursuite d'une finalité légitime, déterminée dans la sphère plus générale de l'objectif légitime mentionné ci-dessus. Cette finalité doit servir un besoin, pour la société, lequel doit être démontré.
- Quatrièmement, les limitations de libertés doivent être réduites au strict minimum pour atteindre la finalité prévue. Ceci implique tant une minimisation des impacts sur les droits fondamentaux que la mise en place de garanties et de mesures de sauvegarde telles que la transparence, la prévisibilité et des contrôles indépendants.

Les principes de finalité légitime et déterminée d'une part et d'efficacité d'autre part forment ensemble le principe de « nécessité ». Le principe de strict minimum, qui implique minimisation et mise en place de garanties contre l'arbitraire, forme le principe de « proportionnalité ». Dans la présente étude, nous analysons la question de la base légale sous le principe de proportionnalité, car elle en est l'une des composantes, en ce qu'elle assure la prévisibilité et une sorte de « transparence contraignante » pour la personne qui restreint les droits fondamentaux d'une autre personne. Dans le même esprit, nous analyserons le principe de but légitime en tant qu'élément de l'exigence de nécessité car il est fondamentalement l'une de ses composantes.

La conformité à l'ensemble de ces exigences doit faire l'objet d'une supervision, de la part d'un parlement ayant des pouvoirs de décision effectifs et de juges indépendants qui peuvent être saisis par les individus concernés. Sortir de ce chemin, dont chaque terme est de la plus grande importance, implique de prendre une route qui conduit inexorablement, à un moment, au totalitarisme. Rester sourd à cette alerte ne peut que masquer un déni de l'histoire, ainsi que l'ont rappelé d'éminents spécialistes, des cours constitutionnelles et des cours suprêmes.

Ces principes s'appliquent à tous les droits et libertés qui sont en jeu lorsque des technologies de surveillance sont utilisées, sauf lorsque la CEDH ou la Cour européenne des droits de l'Homme (Cour EDH) prévoient des conditions plus restrictives. Ces droits sont le droit à la vie privée et à la vie de famille, le droit à la protection des données à caractère personnel, le droit à la liberté d'expression, le droit à la liberté de réunion et d'association, le droit à la liberté d'opinion, le droit à la liberté de circulation, le droit à la liberté physique, le droit de ne pas subir de discrimination, le droit à l'éducation, le droit à un procès équitable, le droit à la dignité et à l'auto-détermination, et le droit de résister à l'oppression.

Sous-section 4.2 : La législation de l'Union européenne

Au niveau de l'Union européenne, la Charte des droits fondamentaux (CDFUE) offre la même protection que la CEDH, en terme de signification et d'étendue, aux droits qu'elle protège et qui figurent aussi dans la CEDH. La protection des données à caractère personnel est précisée dans le règlement de l'UE sur la protection des données à caractère personnel (RGPD), qui s'applique à tous les types de traitements de données personnelles, à l'exclusion des activités strictement personnelles et des traitements effectués par l'autorité judiciaire. Les traitements de données effectués par les cours et tribunaux ainsi que par les services de police sont réglementés par la directive appelée « Police-Justice ». Cette dernière et le RGPD ne s'appliquent pas aux activités des services en charge de la sécurité nationale. Ceci étant dit, les exigences de la CEDH leur demeurent applicables.

Parallèlement à ces instruments qui organisent la protection des données personnelles, l'Union européenne a adopté une série de textes qui imposent aux États de collecter des identifiants

biométriques pour des besoins de contrôle des migrations. La liste des objectifs de cette législation a ensuite été étendue.

En outre, le 21 avril 2021, la Commission européenne a publié une proposition visant à établir des règles harmonisées concernant l'intelligence artificielle (IA). Cette proposition de « législation sur l'intelligence artificielle » encadre la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA dans l'Union. Dans le même temps, elle différencie entre les usages de l'IA qui créent (i) un risque inacceptable, (ii) un risque élevé, et (iii) un risque faible ou minimal. En particulier, la proposition de régulation considère que les systèmes d'identification biométrique à distance « en temps réel » et « a posteriori » devraient être considérés comme présentant un risque élevé et que, en conséquence, ils devraient être soumis à des exigences spécifiques en termes de capacités de journalisation et de contrôle humain. Par ailleurs, la proposition de régulation interdit par principe l'utilisation de systèmes d'identification biométrique à distance « en temps réel » dans les espaces accessibles au public à des fins répressives. Toutefois, cette interdiction peut être remise en cause par la loi nationale dans le cadre de certaines limites et sous réserve qu'une série de mesures de sauvegarde soit mise en place. En outre, l'interdiction ne s'applique pas aux identifications « a posteriori ». Elle ne s'applique pas non plus aux identifications à distance « en temps réel » et « a posteriori » qui seraient effectuées par le secteur privé ou par les autorités publiques pour des besoins de défense nationale.

SECTION 5 : IMPACTS DE L'UTILISATION DE TECHNOLOGIES DE SURVEILLANCE DE MASSE SUR LES DROITS DE L'HOMME

Sous-section 5.1: Les sources d'impact sur les droits de l'Homme

Les sources d'impact sur les droits de l'Homme sont les actions, comportements ou initiatives qui limitent l'exercice de ces droits. Par exemple, le simple fait de collecter des identifiants biométriques limite le droit à la protection des données personnelles. Les impacts sur les droits de l'Homme doivent être conformes aux exigences établies dans la CEDH, la CDFUE et les autres lois de l'UE et nationales qui appliquent ces exigences à des domaines spécifiques, tel que le RGPD. Ces exigences diffèrent selon le droit de l'Homme concerné. Certains droits fondamentaux sont considérés comme absolus et ne peuvent souffrir aucune limitation. C'est le cas de la liberté d'avoir une conviction. D'autres droits fondamentaux sont considérés comme conditionnels et ils peuvent être limités dans de strictes conditions. C'est le cas du droit à la liberté physique. Un dernier groupe de droits fondamentaux peut être limité en suivant l'exigence générale de nécessité et de proportionnalité.

Les impacts sur les droits fondamentaux qui sont conformes aux règles précisées ci-dessus sont considérés légitimes et, sur le fondement de la CEDH, légaux. Les impacts sur les droits fondamentaux qui ne sont pas conformes à ces règles sont considérés arbitraires, et ils constituent une violation du droit fondamental qu'ils restreignent. Ils constituent une violation en eux-mêmes, même si la personne dont les droits sont limités n'en souffre pas, psychologiquement ou physiquement. En effet, ces exigences ne protègent pas seulement les individus, mais également les règles démocratiques et l'État de droit, en imposant à chacun de respecter les droits des autres.

Les impacts illégaux sont ceux qui doivent être identifiés et empêchés. L'identification de ces impacts se déroule en deux phases. La première phase consiste à vérifier que les pratiques connues et la loi sont conformes aux principes de limitation des droits fondamentaux. Dans la présente étude, nous

limitons cette analyse à la conformité aux exigences de nécessité et de proportionnalité, car elles s'appliquent au droit à la protection de la vie privée qui est le premier droit impacté par l'usage de technologies biométriques. Le droit à la protection de la vie privée, lui-même, offre protection à la dignité, à l'auto-détermination et à une série d'autres droits tels que celui à la liberté d'expression et celui de ne pas être le sujet de discrimination. La seconde phase consiste à analyser les risques pour les droits et libertés, afin de s'assurer que tous les impacts potentiels, même indirects, ont été identifiés.

Sous-section 5.2 : Analyse de la conformité de l'utilisation des technologies de surveillance de masse avec l'exigence de nécessité et de proportionnalité

Cette analyse se concentre sur trois textes juridiques, au delà des pratiques de reconnaissance biométrique : la régulation (UE) 2019/1157 qui impose la création de cartes d'identité biométriques, le décret français n° 2016-1460 qui crée une base nationale d'identifiants biométriques et la proposition de législation sur l'intelligence artificielle du 21 avril 2021. Ces trois textes échouent au test de nécessité et de proportionnalité.

Premièrement, ces textes et pratiques présentent un défaut de spécification de leurs finalités. En particulier, les finalités mise en avant dans les textes de droit sont bien trop larges et, dès lors, ne respectent pas l'exigence de finalité déterminée, spécifique et « pressante ». En outre, plusieurs pratiques de détournement de finalité conduisent à l'extension du périmètre d'application de lois une fois qu'elles ont été adoptées, et à la possibilité d'utiliser, dans le cadre de n'importe quelle procédure pénale, une preuve dont l'utilisation aurait du être restreinte à la défense d'une finalité très importante, telle que la lutte contre le terrorisme.

Deuxièmement, l'UE et les États membres ont échoué à démontrer l'efficacité de la législation et des pratiques examinées, malgré de nombreuses demandes en ce sens. En particulier, les autorités publiques n'ont pas démontré, jusque là, la mesure dans laquelle les dispositifs qu'elles proposent sont susceptibles d'apporter à la lutte contre le terrorisme, la criminalité et la fraude.

Troisièmement, la législation et les pratiques examinées sont disproportionnées. La proportionnalité est complexe à évaluer lorsque les finalités, l'efficacité et la plus value des lois et des pratiques ne sont pas connues. Toutefois, même sans cette information, il semble très difficile de soutenir que les traitements de données qui sont proposés ne vont « *pas au-delà de ce qui est nécessaire pour atteindre le but légitime poursuivi* », pour citer le Groupe de travail « Article 29 » sur la protection des données. En particulier, avant cette législation, la gestion des cartes d'identité, la possibilité de passer les frontières et la lutte contre le terrorisme étaient déjà effectives. En rapport, les mesures qui nous occupent concernent l'ensemble de la population, avant toute tentative de commettre une action interdite, sur la base du traitement de données personnelles qui sont parmi les plus sensibles, aux côtés des informations d'ADN.

Quatrièmement, la législation et les pratiques examinées souffrent d'un manque de garanties suffisantes contre l'arbitraire.

La base légale qui établit des restrictions de libertés doit être conforme à la législation nationale et internationale applicable. Pourtant, les actes législatifs de l'UE qui sont examinés se basent sur des dispositions du traité sur le fonctionnement de l'Union européenne (TFUE) qui ne couvrent, en réalité, ni la possibilité d'adopter des dispositions imposant des identifiants biométriques dans les

cartes d'identité, ni la possibilité d'adopter des dispositions autorisant les États membres à utiliser des technologies de reconnaissance faciale dans les lieux publics.

En outre, adopter une loi en conformité avec les règles démocratiques implique en principe qu'une loi soit discutée et adoptée par un parlement doté d'un réel pouvoir de décision. Pourtant, dans certains pays, les pouvoirs du parlement sont affaiblis par différents mécanismes qui, souvent, relèvent de problèmes de séparation des pouvoirs. Par ailleurs, les dispositions qui impactent les droits de l'Homme dans des objectifs de sécurité ou de répression des infractions sont souvent prises en méconnaissance de précédentes opinions qui s'y opposaient, émises par des parlementaires et des autorités légitimes telles que des autorités de protection des données personnelles et des cours suprêmes ou constitutionnelles. Ceci, tant aux niveaux nationaux qu'au niveau de l'Union européenne. Il s'agit d'une situation préoccupante, car elle signifie que les gouvernements et les institutions de l'Union européenne ne respectent pas les contre-pouvoirs qui ont été mis en place afin d'assurer le bon fonctionnement démocratique des systèmes politiques. Pire, cela signifie que les parlements acceptent souvent de légiférer conformément au souhait du gouvernement.

L'opposition parlementaire, et plus largement l'opposition des citoyens, est encore un peu plus affaiblie par la forme de communication qui est pratiquée par les pouvoirs publics depuis au moins deux décennies. Cette communication promeut la sécurité au premier rang des libertés, fait usage d'affirmations très contestables qui stigmatisent les personnes qui s'opposent aux opinions gouvernementales, et utilisent un vocabulaire qui présente les restrictions de droits comme des mesures de protection de ces mêmes droits.

Ces observations sont de la plus grande importance car des garanties démocratiques contre l'arbitraire ne peuvent être prévues que par des lois qui sont adoptées dans le respect des règles démocratiques. Lorsque ces règles sont ignorées, les dispositions de droit qui sont adoptées dans ce contexte ne peuvent pas être présumées proportionnées.

Sous-section 5.3 : Risques pour les droits de l'Homme

Les risques pour le droit à la vie privée consistent en premier lieu en une perte disproportionnée, pour l'individu, d'opacité. En effet, la conservation généralisée et indiscriminée d'identifiants biométriques, de même que la surveillance indiscriminée des lieux accessibles au public, avant que toute infraction n'ait été commise, constituent, en elles-mêmes, une violation du droit à la vie privée. La Cour EDH a rappelé à de nombreuses reprises qu'il doit y avoir un lien entre la conduite d'une personne dont les données sont collectées et les objectifs de la loi qui prévoit cette collecte, afin que la surveillance soit autorisée. Aucun argument ne peut être opposé à cette règle dans une démocratie politique régie par la primauté du droit. En particulier, la préservation de la sécurité intérieure n'est pas une justification suffisante, ainsi que la rappelé la Cour EDH.

Les risques pour le droit à la vie privée incluent une perte injustifiée de développement personnel et d'autonomie personnelle. En effet, les individus qui se sentent surveillés ont une tendance à s'autocensurer, et donc à modifier leur comportement ou à éviter de rencontrer quelqu'un dans un lieu accessible au public. Il est important de rappeler que cet impact existe indépendamment du fait que les individus concernés en souffrent, physiquement ou psychologiquement.

Les risques pour le droit à la vie privée incluent également une menace réelle, actuelle et sérieuse pour l'auto-détermination individuelle et la dignité, alors que ces deux droits ne peuvent recevoir aucune limitation dans une démocratie régie par la primauté du droit. Les données collectées par

surveillance visuelle et acoustique, de même que les caractéristiques biométriques qui sont utilisées pour identifier ou catégoriser les personnes, touchent aux corps et à l'esprit humains. Par conséquent, elle peuvent notamment révéler un nombre important d'informations très intimes, qui en outrent peuvent être faussées. Ces catégories de données font particulièrement courir le risque, lorsqu'elles sont traitées, de conduire à une *« donnéisation ('datafication') des êtres humains* » (Christiane Wendehorst and Yannic Duller), qui entraine plusieurs impacts potentiels. Un premier impact est le risque d'être traité avec un niveau de respect moins important, comparé aux situations dans lesquelles des décisions sont prises hors de tout traitement de données à caractère personnel. Un autre impact possible, pour la personne concernée, est le risque d'être soumise à une décision illégitime, sans aucune possibilité d'y échapper.

Le plus grand risque, sur les terrains du droit à la liberté d'expression et du droit à la liberté de réunion est l'autocensure, comme l'ont montré plusieurs spécialistes et autorités légitimes incluant le CEPD (EDPB), le Conseil de l'Europe et la Cour suprême Allemande. Il est important de rappeler que la liberté d'expression est l'un des « *fondements essentiels* » de la démocratie et de l'État de droit ainsi que « *l'une des conditions primordiales de son progrès* », selon la Cour EDH, et les États ont l'obligation positive d'en assurer l'effectivité. Cela implique que les citoyens aient confiance en la possibilité de s'exprimer sans peur, ce qui interdit de les surveiller lorsque cela n'est pas dûment justifié, nécessaire et encadré. Cela implique également, pour les autorités publiques, l'obligation de ne pas communiquer d'une manière qui stigmatise les personnes qui portent des points de vues contraires aux leurs.

Les risques menaçant le droit absolu d'avoir des convictions sont simplement inacceptables. Les technologies qui identifient ou déduisent les émotions ou les pensées des individus manipulent ces personnes ou induisent leur autocensure. Cet impact est contraire au droit d'avoir des convictions, qui est un droit absolu. Par conséquent, ces technologies ne peuvent pas être utilisées sans le consentement informé des personnes concernées, y compris dans la poursuite d'objectifs liés à la sécurité intérieure ou à la répression des infractions pénales.

Les risques liés aux erreurs et aux vols d'identifiants biométriques sont nombreux.

Les erreurs techniques sont communes. La technologie est susceptible de reconnaître ou d'authentifier une personne par erreur (dans ce cas, on parle de « *fausse concordance »*), ou de ne pas reconnaître ou authentifier une personne alors qu'elle le devrait (ce cas est appelé « *fausse non-concordance*"). Un exemple remarquable d'erreurs dues à une fausse concordance est fourni par un rapport indépendant, qui conclut que le système de reconnaissance faciale utilisé par la police métropolitaine de Londres est « *précis, de manière vérifiable, dans seulement 19% des cas »*, ce qui signifie que « *81% des 'suspects' repérés par* [la] *technologie* [sont] *innocents* ».

Les erreurs et faiblesses humaines sont également courantes. La définition des catégories utilisées pour détecter, évaluer ou classifier les personnes est humaine et subjective. En conséquence, cette définition est sujette à erreurs. La manière dont la technologie est mise en œuvre peut elle-même être source d'impacts non souhaités, tel que le renforcement de stéréotypes. Il pourrait être également argumenté que le choix de la biométrie et de la vidéo-surveillance pour répondre à un objectif de sécurité est, en lui-même, une erreur humaine de trajectoire. En effet, l'identification biométrique n'apporte aucune sécurité. Elle permet uniquement, éventuellement, d'identifier des personnes déjà suspectées de préparer une infraction. Ce pourrait être la raison pour laquelle la recherche biométrique se concentre sur la prédiction. Par contre, dans une société démocratique

régie par la primauté du droit, la restriction d'une liberté sur la base d'une prédiction des comportements n'est pas admissible. Elle constitue, en elle-même, une violation du droit d'avoir une conviction, du droit à l'auto-détermination et du droit au libre-arbitre. Au final, elle constitue une violation de la dignité humaine. Ce principe s'applique également à l'industrie.

Les risques de vol d'identifiants biométriques sont également élevés. Les données biométriques peuvent être vulnérables aux risques à quatre niveaux. Au niveau de l'individu, le vol d'empreintes digitales ou de caractéristiques faciales est assez facile, et ceci est de plus en plus documenté. Les identifiants biométriques peuvent aussi être interceptés lorsqu'ils sont capturés, transmis ou comparés à la base de données principale. Dans les systèmes d'authentification standards, si les règles de base de la sécurité sont respectées, l'impact d'un vol à ces trois derniers niveaux est généralement plutôt réduit. Inversement, le vol d'un identifiant biométrique peut avoir un impact extrêmement important. En effet, cet identifiant est réutilisable, par conception, sur tout autre système basé sur la biométrie, dans la poursuite d'objectifs multiples, sans que la personne concernée ne soit nécessairement consciente de cette utilisation abusive.

Les risques d'erreur et de vol entraînent, en pratique, un renversement de la charge de la preuve. Les erreurs humaines et techniques sont particulièrement inquiétantes lorsqu'elles concernent des identifiants biométriques, car ces identifiants sont présentés comme extrêmement fiables. La victime d'une erreur d'identification est donc susceptible de devoir, en pratique, démontrer cette erreur. Pourtant, dans le système juridique gouverné par la CEDH, la charge de la preuve de la nécessité et de la proportionnalité d'une restriction de liberté repose sur la personne qui impose cette restriction. Ce renversement de la charge de la preuve constitue une violation de la CEDH.

Les risques d'erreur et de vol impactent le droit à un procès équitable et le droit à la dignité humaine. En premier lieu, la surveillance des lieux accessibles au public remet en cause la présomption d'innocence, puisqu'elle conduit à stigmatiser, par défaut, tout individu en tant que suspect. Yves Poullet observe également que cette représentation négative de l'être humain peut au final conduire à induire des comportements qui, ensuite, justifieront le système de surveillance. Ceci heurterait directement l'auto-détermination humaine et la dignité humaine. En outre, l'utilisation de ces technologies remet en cause le principe selon lequel les infractions et les peines doivent être définies par la loi, puisque les facteurs qui sont surveillés ne sont généralement pas connus. Finalement, l'utilisation d'identifiants biométriques a des impacts sur la dignité car elle induit la possibilité qu'un grand nombre de personnes accède à ces identifiants, privant ainsi l'individu de la possibilité de choisir par qui et pourquoi ses identifiants peuvent être utilisés. Ceci prend place dans un contexte où chaque accès indu peut avoir de terribles conséquences, puisque l'identifiant ne peut pas être révoqué. Ceci prend également place dans un contexte où la mauvaise gestion de bases de données biométriques publiques, nationales et européennes, a été démontrée.

L'utilisation d'identifiants biométriques pour des raisons de sécurité, et plus précisément pour combattre le terrorisme et gérer les frontières, impacte également la crédibilité même de la lutte contre le terrorisme. En effet, il en résulte une discrimination des personnes sur la base de leur nature, caractère, apparence, ou origine sociale ou ethnique. Il existe une contradiction explicite à combattre le terrorisme au nom de valeurs qui incluent le droit à la non-discrimination, en utilisant des méthodes discriminatoires basées sur des caractéristiques ethniques et sociales. Dans le même sens, François Sureau souligne que l'atteinte disproportionnée qui est portée aux libertés au nom de la lutte contre le terrorisme offre à ce dernier « *une victoire sans combat, en montrant à quel point*

nos principes étaient fragiles ». Ces contradictions discréditent la lutte contre le terrorisme au nom des valeurs européennes.

L'utilisation de technologies biométriques permettant la surveillance de masse est, *in fine*, une source de risque pour la démocratie elle-même. En premier lieu, cette utilisation induit une possibilité d'abus qui n'a jamais été atteinte dans l'histoire. Elle menace le droit à l'auto-détermination et le droit à la dignité humaine, qui ne souffrent aucune restriction dans une démocratie respectueuse de l'État de droit, puisqu'ils constituent déjà le cœur des droits fondamentaux, qui doit être respecté en toute circonstance. Malgré cette situation, l'Union européenne et plusieurs États membres ferment les yeux et font la sourde d'oreille aux analyses juridiques, opinions des autorités de protection des données personnelles et décisions de justice qui soulignent l'inacceptabilité des pratiques. Cette circonstance pourrait constituer le signal clair d'une attitude de « *prise de décision paternaliste 'dans les meilleurs intérêts'* » d'autrui, pour citer la Cour EDH, qui serait inacceptable.

L'un des impacts les plus évidents de cette situation est le risque de disparition du droit de résistance à l'oppression. Cela a notamment été souligné par cent vingt membres du Parlement français en 2012, en lien avec la création d'une base centralisée de données biométriques, qualifiée de « *fichier des gens honnêtes* ». En substance, une telle disparition signifierait que la démocratie libérale elle-même a déjà disparu. Cela signifierait que le cœur des droits fondamentaux a lui-même disparu – en raison d'une négation des éléments constitutifs de la démocratie que sont les exigences de nécessité et de proportionnalité de toute restriction de droit.

SECTION 6: RECOMMANDATIONS

La présente analyse nous conduit à formuler quatre recommandations qui paraissent indiscutables si l'Union européenne et ses États membres entendent rester sur la voie démocratique. Elles peuvent être résumées de la manière proposée ci-dessous.

1. Organiser des états généraux de la démocratie, des droits de l'Homme et de l'État de droit

Une protection des droits de l'Homme adaptée implique que des analyses de nécessité et de proportionnalité d'une part, et que des analyses de risque d'autre part, soient conduites de manière appropriée. Elle implique également que la loi adoptée pour servir de fondement aux pratiques soit conforme aux exigences de base légale claire et légitime. Ceci ne peut être assuré que dans les États dans lesquels les contre-pouvoirs démocratiques sont effectifs. Actuellement, cela ne semble pas être le cas, tant au niveau des institutions de l'Union européenne qu'au niveau de certains de ses États membres.

Par conséquent, il apparaît crucial de conduire une évaluation effective du bon fonctionnement démocratique des institutions européennes et des États membres de l'Union européenne, ainsi que d'assurer que ces derniers entreprennent les réformes nécessaires pour restaurer des contre-pouvoirs effectifs et ainsi se conformer aux principes de l'État de droit. En particulier, les parlements doivent être dotés d'un pouvoir de décision effectif et ne doivent pas être contournés. Les cours de justice doivent être indépendantes et leurs décisions doivent être appliquées. Les autorités de protection des données personnelles doivent avoir des pouvoirs de décision et de contrôle effectifs et leurs décisions doivent être appliquées également. Toutes ces autorités et institutions doivent recevoir les équipements et ressources nécessaires à l'exercice de leurs missions.

2. Restaurer les conditions du débat démocratique

Dans une démocratie politique, les États doivent assurer la mise en place des meilleurs paramètres contextuels permettant le débat public. Ils doivent également assurer la prise en compte des opinions contraires. Les autorités publiques et les représentants politiques ont une responsabilité particulière de s'assurer qu'ils agissent conformément aux choix des citoyens, en particulier lorsque des voix s'élèvent contre un risque pour des droits fondamentaux absolus.

Restaurer les conditions du débat démocratique implique également d'éviter les présentations erronées de la réalité, y compris concernant le véritable contenu des dispositions législatives qui fondent la préservation des droits de l'Homme. La manipulation des sondages d'opinion devrait être interdite et la forme de la communication publique, elle-même, devrait ne stigmatiser ni les minorités, ni les autorités et les personnes qui remettent en cause la légitimité de propositions gouvernementales. Des codes de conduite destinés aux représentants politiques et publics pourraient être envisagés dans un objectif de promouvoir une « *éthique de la communication* » (Commission de Venise).

3. Mettre en place une éducation aux droits de l'Homme au sein de la société et dans la sphère politique, aux niveaux nationaux et de l'Union européenne

La démocratie exige que les citoyens comprennent ce que la législation et les pratiques impliquent réellement. Ceci suppose notamment de les doter des compétences et de l'attitude critique nécessaires qui leur permettent de faire face à l'information qu'ils reçoivent et de la comprendre. Ce droit à l'éducation est d'une importance particulière comme l'ont particulièrement souligné le Comité des ministres du Conseil de l'Europe et le Parlement européen.

Une culture des droits de l'Homme doit également être favorisée auprès des représentants politiques et publics, aux niveaux nationaux mais également au niveau de l'Union européenne. En effet, dans une société démocratique respectueuse de l'État de droit, il n'est pas acceptable que ces représentants tiennent des propos et entreprennent des actions qui contredisent directement la lettre et l'esprit des textes qui préservent les droits de l'Homme. Ces pratiques et déclarations démontrent un manque de culture de la démocratie et des droits de l'Homme.

La compréhension de la lettre et de la philosophie de préservation des droits de l'Homme devrait également imprégner les analyses d'impact sur la vie privée et les données personnelles (respectivement AIVP et AIDP), qui actuellement réduisent souvent l'analyse de nécessité et de proportionnalité à une vérification de conformité au RGPD ou à la directive Police-Justice.

4. Déclarer un moratoire immédiat concernant les technologies et pratiques qui impactent le droit d'avoir des convictions, le droit à l'auto-détermination, le droit à la dignité humaine et le droit de résister à l'oppression

Différents usages d'identifiants biométriques constituent une violation, ou induisent des risques intolérables, pour une série de droits absolus tels que le droit d'avoir une conviction, le droit à l'auto-détermination, le droit à la dignité humaine et le droit de résister à l'oppression. Cette situation entraîne un risque pour la démocratie libérale en tant que régime politique. Par conséquent, il est crucial que ces pratiques soient interdites, le temps requis pour mettre en place les conditions nécessaires à leur évaluation démocratique, de conduire cette évaluation et d'en soumettre les résultats à un débat public approprié.

Les méthodes de traitement de données les plus dangereuses pourraient être discriminées des autres méthodes sur la base des trois critères suivants : (1) la proximité du stockage de données par rapport à la personne concernée ; (2) les possibilités de réutilisation de l'identifiant biométrique à d'autres fins ; et (3) la précision de l'identifiant biométrique.

Les technologies et pratiques devant être prohibées dans un premier temps incluent les suivantes :

(1) La collecte et le traitement, par les États et par les institutions de l'Union européenne, des identifiants biométriques relatifs à l'ensemble des citoyens d'une part et à l'ensemble des migrants d'autre part, sans autre discrimination nécessaire et proportionnée fondée sur la démonstration de besoins réels et cruciaux.

(2) La collecte et le traitement, par des entités privées, d'identifiants biométriques sans le consentement libre, spécifique, explicite et informé des personnes impliquées. Cela couvre la collecte de photographies et d'autres identifiants biométriques qui sont disponibles publiquement ou qui sont disponibles sur Internet.

(3) La reconnaissance faciale dans les espaces accessibles au public.

(4) La reconnaissance et la classification biométrique et comportementale sans le consentement libre, spécifique, explicite et informé des personnes concernées. En outre, ces technologies ne doivent pas conduire à prendre des décisions à l'encontre des personnes impliquées ou à l'encontre de tout autre être humain sans un consentement de même nature formulé par les personnes concernées ou impliquées.

Dans chacune et dans toutes ces situations, les technologies et services autorisés devraient être soumis à une analyse d'impact sur la vie privée appropriée, et leur responsable devrait être capable de démontrer que les conclusions de cette analyse, en termes de mesures correctrices et de garanties à prévoir, ont été mises en œuvre et seront régulièrement soumises à un contrôle indépendant.

8. CONCLUSION

Depuis près de vingt ans, la biométrie est présentée comme un moyen indiscutable d'assurer la sécurité des personnes, tant dans la sphère publique que dans leur sphère privée. Sur cette seule base, les États européens mettent en oeuvre, de manière croissante, des technologies intrusives, sans même avoir été capables de démontrer leur efficacité et leur plus-value, malgré les demandes continues en ce sens.

Inversement, une analyse des enjeux en présence démontre d'importants risques de fraude ainsi que des risques d'erreur humaine et technique, illustrés de cas concrets. Ces observations interviennent dans un contexte où la mauvaise gestion des bases de données déjà existantes, aux niveaux nationaux et de l'Union européenne, a été démontrée. En outre, une analyse juridique rigoureuse met à jour des risques intolérables pour des droits et libertés qui sont aux fondements de toute démocratie politique qui se soucie de respecter ses membres. En particulier, cette analyse démontre que le simple vol d'un identifiant biométrique ou le détournement de finalité d'un traitement de données biométriques peut avoir des impacts très importants sur les individus, en plus d'affecter leur dignité sur la base d'un traitement de données non consenti et portant malgré tout sur une information des plus intimes.

Les véritables raisons de cette situation Kafkaïenne ne sont pas évidentes. L'industrie biométrique y joue sans aucun doute un rôle. La tentation, inhérente à tout État, d'assurer l'ordre interne, s'y surajoute certainement. Quoi qu'il en soit, cette situation est rendue possible par l'affaiblissement des contre-pouvoirs démocratiques et une perversion de la communication publique, qui recherche l'acceptabilité au détriment de la justification. Ceci peut être observé tant au niveau de l'Union européenne que de ses États membres. En d'autres termes, cette situation est le résultat d'un abandon pratique des principes que tous les États membres se sont pourtant engagés à respecter à l'issue de la seconde guerre mondiale au sein du Conseil de l'Europe, afin de prévenir le retour d'un régime totalitaire.

Les États membres de l'Union européenne se trouvent dès lors aujourd'hui confrontés à un choix politique crucial. Le choix de renouer avec les principes et les valeurs de l'État de droit et de respect des droits de l'Homme, ou le choix de sortir de ce chemin pour emprunter la route du totalitarisme. Cette affirmation n'est pas exagérée, elle est pragmatique. Elle sera comprise par quiconque s'est penché sur l'histoire et est conscient de la pertinence et de la valeur des principes que nous ont transmis les rédacteurs de la Convention européenne des droits de l'Homme. Elle sera comprise par quiconque a pris connaissance des appels à interdire les technologies biométriques, de la part de presque tous les contre-pouvoirs qui subsistent: les Nations Unies, le Parlement européen, les autorités de protection des données personnelles et les organisations non-gouvernementales qui travaillent au quotidien à la préservation des droits de l'Homme.

Plus cette décision sera tardive, moins elle sera facile à mettre en œuvre, lorsque toutes les technologies seront en place.

Pour emprunter des mots[3] prononcés il y a plus de vingt ans par l'actuel président du Conseil des barreaux européens (CCBE), la question qui est posée aux États et aux institutions de l'Union européenne est celle de savoir s'ils sont capables de démontrer leur « *maturité démocratique* ». Plus spécifiquement, la question est de savoir s'ils ont admis « *la primauté de l'Homme* » ou s'ils exigent « *sa soumission* ».

[3] Michel Bénichou, « Le résistible déclin du secret », LPA, 20 juin 2001, n°122, p. 3 s.

La réponse à cette question, dans le cadre des arguments à opposer au terrorisme, sera sans aucun doute décisive.