La vie privée à l'épreuve de la société numérique

Jacques Chevallier

LA VIE PRIVÉE
A L'ÉPREUVE DE LA SOCIÉTÉ NUMÉRIQUE

Jacques Chevallier
Professeur émérite de l'Université Panthéon-Assas (Paris 2)
CERSA-CNRS

In Penser le droit à partir de l'individu. Mélanges en l'honneur d'Elisabeth Zoller, Dalloz, 2018, pp. 563-576

La révolution numérique est un processus global, qui s'étend à tous les aspects de la vie sociale : organisation des activités productives et conception du travail, accès à la culture et à l'enseignement, loisirs et comportements sociaux, relations de pouvoir et fonctionnement des organisations… [1] ; tout se passe comme si une société nouvelle était en passe d'émerger, la numérisation mettant en cause l'ensemble des équilibres économiques, sociaux et politiques, en produisant une authentique rupture (« disruption »). Cette rupture concerne en tout premier lieu la sphère d'autonomie dont disposent les individus, et touche par-là même à la liberté individuelle[2] : si les libertés d'information et d'expression acquièrent à l'ère de la société numérique une portée nouvelle, la numérisation donne aussi des possibilités de collecte, de stockage et d'exploitation des données personnelles sans commune mesure avec celles qui existaient auparavant ; l'idée de « vie privée » tend ainsi à perdre une part au moins de sa consistance.

La prise de conscience des dangers qui pouvaient résulter notamment de la connexion des fichiers détenus par les administrations a sans doute entraîné l'établissement dès 1978 en France, avec l'adoption de la loi « Informatique et libertés », d'un régime de protection précurseur. La transposition en 2004 de la directive européenne du 24 octobre 1995 n'a modifié ce régime qu'à la marge : l'élargissement du champ d'application de la loi, qui vise l'ensemble des traitements, automatisés ou non, privés ou publics, de « données à caractère personnel » (l'expression se substituant à celle d' « informations nominatives ») est assorti de la consolidation du système de protection et du renforcement des pouvoirs de l'autorité indépendante de contrôle (la CNIL) ; les règles posées, concernant le traitement de ce type de données (interdiction de la collecte de données sensibles, qualité des données recueillies, durée de conservation, principe du consentement de la personne concernée...), étaient censées interdire toute dérive possible.

Ce cadre juridique apparaît désormais insuffisant pour endiguer le mouvement de diffusion des données personnelles dans toutes les sphères de la vie sociale et leur exploitation

---

[1] M. Dugain, C. Labbé, *L'homme nu. La dictature invisible du numérique*, R. Laffont-Plon, 2016. Sur l'impact du développement des plateformes numériques, voir Conseil d'État, « Puissance publique et plateformes numériques » : accompagner l'uberisation », *EDCE*, n° 68, 2017.

[2] On entend ici la notion de « liberté individuelle » au sens large, et non au sens restrictif donné par le Conseil constitutionnel à la notion de « liberté individuelle », qu'il distingue de la « liberté personnelle » (16 juin 1999).

systématique à l'aide de nouveaux outils : l'affaire Snowden a révélé l'accès dont disposaient les services de renseignement des différents États sur les communications électroniques ; et le croisement des données personnelles est devenu la règle, tant pour la mise en œuvre des politiques publiques que pour la fourniture des biens et services. La nécessité de repenser le système de protection des données personnelles, que l'évolution des techniques et des usages a rendu en partie obsolète, est désormais admise, aussi bien au niveau national qu'au niveau européen : tandis que le Conseil d'État s'est efforcé en 2014[3] de définir les principes devant fonder « la protection des droits fondamentaux à l'ère du numérique », la loi du 7 octobre 2016 « Pour une République numérique » a entendu, tout en favorisant « la circulation des données et du savoir », assurer une meilleure protection des droits ainsi que faciliter l'accès au numérique ; quant au règlement européen du 27 avril 2016 sur la protection des données, qui sera applicable à partir du 25 mai 2018, il apporte des changements majeurs concernant la notion de données personnelles, les conditions de leurs collecte et le dispositif de sanction. Si elles sont sans nul doute importantes, ces garanties nouvelles apparaissent néanmoins insuffisantes pour contrebalancer la dynamique qui, sous l'influence de facteurs variés, pousse à un accès toujours plus large et à une exploitation toujours plus intensive des données personnelles.

Les possibilités offertes par la numérisation des données conduit à une *société de surveillance,* dans laquelle les individus sont placés sous le regard vigilant des autorités publiques, et à une *société de contrôle,* dans laquelle une emprise insidieuse parce qu'invisible est exercée sur les comportements.

I. LA NUMÉRISATION COMME INSTRUMENT DE SURVEILLANCE

Si l'idée de surveillance est inhérente à l'institution même de l'État, la police ayant pour mission de prévenir les atteintes à l'ordre public, elle a pris dans les sociétés contemporaines une dimension nouvelle. L'importance croissante prise par le thème de la sécurité[4], notamment sous l'impact de la menace terroriste, contribue en effet à mettre en avant l'impératif de prévention, au risque de brouiller la distinction traditionnelle entre répression pénale et police administrative[5] : tandis que la réaction pénale tend à s'élargir de « l'infraction commise » à « l'infraction redoutée », en prenant en compte, non plus seulement la « culpabilité » mais encore la « dangerosité » présumée des intéressés, la prévention des différentes formes de délinquance puis la lutte contre le terrorisme vont pousser à étendre toujours davantage les dispositifs de surveillance. Les technologies numériques vont être un instrument privilégié de cette entreprise, en donnant à la police « de nouveaux moyens d'investigation »[6] : leur utilisation visera à détecter, à partir de la collecte systématique et généralisée de données personnelles, des individus « dangereux » ou des comportements « à risque », dans le cadre d'une « sécurisation prédictive »[7] ; on assiste ainsi à la mise en place

---

[3] « Le numérique et les droits fondamentaux », *EDCE,* n° 64, 2014

[4] J. Chevallier, « L'État de droit au défi de l'État sécuritaire », in *Mélanges François Ost*, Presses des Facultés universitaires Saint-Louis, 2017. S

[5] J. Allix, « La lutte contre le terrorisme entre prévention pénale et prévention administrative », in M. Touillier (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?,* Dalloz, Coll. Les sens du droit, 2017, pp. 147 sq.

[6] Conseil d'État, rapport préc. Pp. 25, 116 sq.

[7] Le Département américain de la Sécurité intérieure lancera ainsi en 2007 un programme destiné à identifier les « terroristes potentiels ».

d'une « data surveillance », une surveillance par les données, s'étendant à l'ensemble de la population et poussant très loin la logique intrusive[8].

Déjà présente dans les dispositifs de vidéo-protection qui, en cherchant à détecter des « comportements anormaux », relèvent d'une logique de profilage, la conception élargie de la surveillance prend appui sur la numérisation des fichiers (A) et passe par l'accès aux communications électroniques (B).

A) Les fichiers numérisés

Entendus au sens large comme englobant les divers systèmes ayant pour objet de rassembler et de classer de manière ordonnée et systématique un ensemble de données, les fichier sont nés avec l'apparition de l'État moderne et apparaissant comme inhérents à son essence ; s'ils remplissent plusieurs types de fonctions[9], ils sont utilisés par l'État pour asseoir, via la collecte d'informations nominatives, son contrôle sur tout ou partie de la population. Si des fichiers ont toujours existé, dans un but de police ou en matière fiscale, et si la formule a connu une importante extension avec le développement des interventions sociales, l'informatisation a constitué une authentique rupture : d'une part, la prolifération des fichiers et la capacité de stockage dont ils disposent donne à l'État le moyen de connaître des citoyens dans toutes les facettes de leur existence ; d'autre part, et surtout, les possibilités d'interconnexion de ces fichiers comportent le danger d'un profilage des individus.

1° Les technologies numériques sont d'abord utilisées pour améliorer les moyens d'*identification* des individus. Les modes d'identification par lesquels l'État assure traditionnellement son contrôle sur les populations[10] tendent à être complétés par la collecte de données biométriques : il s'agit de numériser une partie du corps (taille, couleur des yeux, empreintes digitales ou encore d'autres éléments), afin d'établir avec certitude l'identité de la personne, en interdisant toute possibilité de fraude. Un saut qualitatif est franchi dès l'instant où ces données personnelles numérisées ne figurent plus seulement sur un « composant électronique sécurisé » (puce) détenu par les intéressés mais sont enregistrées et stockées dans des *fichiers*. Par application du règlement européen du 13 décembre 2004, le décret du 30 décembre 2005 a ainsi prévu que les passeports comportent un composant électronique, contenant les éléments d'identification des personnes : et le décret du 30 avril 2008 a prévu l'enregistrement des données biométriques dans un fichier national[11], dont l'accès a été encadré par le décret du 19 juin 2015.

Un projet plus général de mise en place d'une « identité nationale électronique sécurisée » (INES), couvrant carte d'identité et passeport et comportant les mêmes éléments biométriques a été élaboré, aboutissant, au prix de vives controverses, à la loi du 27 mars 2012 relative à la protection de l'identité : le texte devait aboutir à la création d'un composant électronique sécurisé intégrant ces éléments ainsi qu'à la mise en place d'un fichier central ; amputé à la suite de la décision du Conseil constitutionnel du 22 mars des dispositions relatives au fichier, au motif que celui-ci pouvait être consulté à d'autres fins que la vérification de l'identité[12], il

---

[8] « L'objectif est de collecter toujours plus d'informations, même les plus insignifiantes, sur un individu, dans l'idée qu'il y aura toujours un algorithme pour en extraire un renseignement utile » M. Dugain, C. Labbé, *op. cit.*, p. 63).

[9] F. Eddazi, S. Mauclair (dir.), *Le fichier*, LGDJ, 2017, p. 127.

[10] X. Crettiez, P. Piazza (eds.), *Du papier à la biométrie. Identifier les individus*, Presses SciencesPo, 2006. A. Mattelart, .A Vitalis, *Le profilage des populations. Du livret ouvrier au cyber contrôle*, La Découverte, 2014.

[11] Dans l'arrêt du 26 oct. 2011, le Conseil d'État a admis la légalité de la création du fichier, se bornant à censurer la collecte et la conservation de huit empreintes de doigts.

[12] Selon le Conseil, un tel fichier porterait au « droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ». La décision du 24 août 2017 par laquelle la Cour suprême de l'Inde a reconnu le caractère fondamental du droit à la vie privée s'inscrit dans la même perspective, en

est resté pendant longtemps bloqué faute de décret d'application. Il a fallu attendre le décret du 28 octobre 2016 pour que soit mis en place un « traitement de données à caractère personnel », dénommé « titres électroniques sécurisés » (TES), couvrant à la fois les passeports et les cartes nationales d'identité et intégrant un ensemble étendu de données à caractère personnel, dont l'image numérisée du visage, des empreintes digitales et de la signature : s'il est prévu que le traitement « ne comporte pas de dispositif de recherche permettant l'identification » à partir de ces données numérisées, un ensemble de services administratifs ont la possibilité d'accéder à ces données dans le cadre de l'exercice de leurs missions. Ce regroupement dans un même fichier d'informations personnelles concernant la quasi totalité de la population et les risques possibles de détournement de ses finalités avaient incité la Commission nationale de l'informatique et des libertés (CNIL) à souhaiter qu'un débat au Parlement ait lieu sur le projet[13] ; le décret du 9 mai 2017 a seulement permis aux demandeurs de refuser la numérisation et l'enregistrement de ses empreintes digitales, celles-ci étant alors recueillies sur un formulaire joint au dossier de demande.

Pour les étrangers résidant en France, un fichier central des étrangers a été mis en place dès 1917 au ministère de l'Intérieur, en liaison avec la création par le décret du 2 avril 1917 d'une « carte nationale d'identité à l'usage des étrangers », avant que ne prolifèrent au cours de la période récente des fichiers spécifiques, au niveau national (fichier des étrangers non admis, fichier des étrangers sollicitant la délivrance d'un visa, fichier dactyloscopique des demandeurs d'asile…) et européen (Eurodac, système d'information Schengen SIS), aboutissant à un véritable « surfichage des étrangers par rapport au reste de la population » ; mais ici l'objectif d'identification se double très explicitement d'une volonté de surveillance.

2° La logique de *surveillance* est plus explicite dans les fichiers de police, dont l'origine est ancienne, mais qui se sont multipliés au cours des dernières années[14] et tendent à être connectés au sein de méga fichiers : après la tentative avortée de mise en place de Safari en 1974, le projet de création en 2008 du fichier EDVIGE (« Exploitation documentaire et valorisation de l'information générale »), conçu à la suite du regroupement de la DCRI, des RG et de la DST, a finalement échoué compte tenu de la montée des oppositions ; mais le fichier EDVIRSP (« Exploitation documentaire et valorisation de l'information relative à la sécurité publique ») a repris l'essentiel de ses ambitions, en supprimant cependant les données relatives à la santé et la vie sexuelle. La lutte contre le terrorisme a justifié plus récemment une floraison de fichiers, notamment pour prévenir la menace djihadiste[15], posant par-là même d'importants problèmes de coordination et de circulation de l'information entre les différents services concernés[16].

Concernant la police judiciaire, le « système de traitement des infractions constatées » (STIC), créé en 1995, qui regroupait déjà un certain nombre de fichiers de police, fusionnera en mai 2012 avec le fichier Judex de la gendarmerie au sein du « Traitement des antécédents judiciaires » (TAJ), qui entend intégrer toutes les données se rapportant à l'environnement

---

impliquant la remise en cause d'un programme étendu de relevé de données biométriques, concernant l'ensemble de la population.

[13] R. Perray, « Le fichier TES : un réel danger ? », *Dalloz*, 2017, pp. 56 sq.

[14] On en comptait déjà 80 en 2012 selon A. MATTELART., A. VITALIS (*Le profilage des populations. Du livret ouvrier au cybercontrôle*, La Découverte, 2014, p. 127 et s.) et depuis lors leur nombre s'est fortement accru.

[15] Tel le « fichier des signalements pour la prévention de la radicalisation à caractère terroriste » (FSPRT) administré par l'UCLAT (Décret du 5 mars 2015 modifié par décret du 2 août 2017) : 17.393 personnes étaient inscrites sur ce fichier au 1er mars 2017..

[16] Le système CHEOPS (« Circulation hiérarchisée des enregistrements opérationnels de la police sécurisée ») créé en 2001 révèlera un certain nombre de faiblesses.

d'un crime, au risque d'étendre démesurément le nombre des personnes fichées[17] ; un fichier spécifique sera créé suite aux attentats de janvier 2015 pour les « auteurs d'infractions terroristes ». Il convient d'ajouter à ces fichiers le « fichier des personnes recherchées » (FPR)[18], dont les possibilités de consultation le « fichier automatisé des empreintes digitales » (FAED), créé en 1987 concernant les individus mis en cause dans des procédures pénales pour crimes et délits, ainsi que le « fichier national automatisé des empreintes génétiques » (FNAEG), créé en 1998 pour lutter contre les criminels sexuels mais dont le champ d'application a été ensuite sensiblement élargi[19].

Les possibilités nouvelles de surveillance offertes par la numérisation des fichiers tendent à être utilisées dans une perspective plus large, comme le montre la question sensible du fichage des passagers aériens (*Passenger Name Record* (PNR). Le débat concernant la mise en place d'un tel système s'est situé à plusieurs niveaux : transatlantique, les négociations entre les Etats-Unis et l'Union européenne ayant été bloquées à plusieurs reprises[20] ; national, un système API-ANR autorisé dès 2006 ayant été relancé en 2014 ; européen enfin, la directive finalement adoptée le 21 avril 2016 (2016/681) après de longues discussions prévoyant un échange de données entre les pays européens, par l'intermédiaire des Unions nationales Information Passagers (UIP) — directive transposée par la loi sur la sécurité intérieure et la lutte contre le terrorisme adoptée fin 2017 (**voir le décret du 3 août 2018**). Le volume des informations collectées est impressionnant, leur délai de conservation est fixé à cinq ans : les déplacements aériens sont désormais placés sous haute surveillance, celle-ci s'appuyant sur un traitement automatique de données visant à faire émerger, par leur croisement, des profils « à risque ».

La logique de surveillance ne prend pas seulement appui sur la numérisation ; elle s'insinue au cœur même du système de communication issu du développement de la société numérique.

B) Les communications électroniques

L'accès aux communications électroniques, échangées par Internet ou par téléphone mobile, qui constituent désormais le moyen privilégié de communication sociale, pousse beaucoup plus loin l'intrusion dans la vie privée. Si cette intrusion est légitimée par la lutte contre le terrorisme, l'absence de profil terroriste type a pour effet d'étendre son champ d'application, au risque de glisser vers une surveillance de masse.

1° Ce pas avait été franchi aux États-Unis après le 11 septembre. Sur la base de la section 215 du *Patriot Act* du 26 octobre 2001 autorisant, au nom de la lutte contre le terrorisme, la collecte et le stockage de ces communications sans mandat judiciaire, avait été mis en place un système d'interception des données mises en ligne, aux Etats-Unis mais aussi à l'étranger, de très grande ampleur par la NSA (*National Security Agency*) : les communications électroniques stockées par l'Agence dans le cadre du programme PRISM pouvaient être ensuite consultées et croisées par les personnes habilitées, à l'aide d'une interface d'utilisation

[17] Dans sa décision du 27 octobre 2017, le Conseil constitutionnel a jugé que l'impossibilité d'effacement des données personnelles pour les personnes n'ayant pas fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classelent sans suite portait « une atteinte disproportionnée au droit au respect de la vie privée ».

[18] Le fichier S est une sous-catégorie de ce fichier. Les possibilités de consultation du FPR ont été élargies (décret du 2 août 2017)

[19] La CEDH a estimé dans un arrêt du 22 juin 2017, *Aycaguer c/France*, que le régime de conservation des profils ADN par le FNAEG n'offrait pas « en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante », rejoignant ainsi les réserves qu'avait formulées le Conseil constitutionnel le 6 septembre 2010.

[20] L'accord du 14 mai 2006 ayant été annulé par la CJUE le 30 mai 2006 et celui du 26 juillet 2007 n'ayant pas été entériné par le Parlement européen. Un nouvel accord, conclu pour sept ans, a été signé en décembre 2011.

XKeystore ; ce système était doublé d'échanges réciproques de données avec les services de renseignement d'autres pays.

Suite à la vive émotion suscitée par les documents révélés par Edward Snowden le 7 juin 2013, ce système de collecte massive, automatique et indiscriminé de données a été remis en cause par l'*USA Freedom Act* adopté par le Sénat le 2 juin 2015, les autorités ne pouvant plus avoir accès aux métadonnées stockées par les opérateurs que ponctuellement et en justifiant d'un lien avec le terrorisme ; mais la limite ainsi posée reste fragile et plus formelle que réelle..

2° Concernant la France, alors que la loi du 10 juillet 1991 n'autorisait la surveillance des communications électroniques que sur décision judiciaire ou « à titre exceptionnel » par décision du Premier ministre sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), une première brèche avait été ouverte par la loi du 23 janvier 2006, prévoyant une procédure de réquisition des métadonnées auprès des fournisseurs d'accès à Internet et des hébergeurs ; en marge de ce texte avait été créé en 2008 un « Pôle national de Cryptanalyse et de Décryptement » (PNCD), permettant de recueillir à partir de câbles sous-marins et de stocker des milliards de données, mis à la disposition, non seulement de la DGSE, mais de l'ensemble des services de renseignement, sans véritable contrôle.

Le cadre légal, désormais intégré dans le code de la sécurité intérieure, a été après 2012 revu et élargi, en plusieurs étapes. D'abord, une possibilité d' « accès administratif aux données de connexion » a été introduite par la loi de programmation militaire du 18 décembre 2013, le décret du 14 décembre 2014 ayant défini les données pouvant être recueillies, dressé la liste des services pouvant y accéder et précisé les conditions de leur transmission et de leur conservation. Puis la loi sur le renseignement du 24 juillet 2015, complétée par la loi du 30 novembre 2015 relative aux communications électroniques internationales, est venue, au nom de la lutte contre les menaces terroristes prévoir de nouvelles techniques, interceptions de sécurité, sonorisation et lieux et de véhicules, captation d'images et de données informatiques, pose de capteurs de communications téléphoniques de proximité (IMSI Catchers) et surtout installation chez les opérateurs de « boîtes noires » visant à détecter, à partir du croisement d'un ensemble de métadonnées, une menace terroriste ; si le recours à ces procédés, qui supposent une autorisation du Premier ministre, après avis de la nouvelle « Commission nationale de contrôle des techniques de renseignement » (CNCTR), est justifié par la « prévention du terrorisme », le système des boîtes noires pourra notamment être considéré comme permettant la « collecte de manière indifférenciée d'un volume important de données qui peuvent être relatives à des personnes tout à fait étrangères à la mission de renseignement »[21], et donc comme l'esquisse d'une surveillance de masse[22]. Enfin, l'extension à l'entourage des suspects des possibilités de collecte des données de connexion dans le cadre d'enquêtes liées au terrorisme, qui figurait dans la loi du 21 juillet 2016 (art. 15) de prorogation de l'état d'urgence[23], a été pérennisée par la loi du 30 octobre 2017 « renforçant la sécurité intérieure et la lutte contre le terrorisme »[24], le texte prolongeant par ailleurs la possibilité d'installation des boîtes noires précitées.

---

[21] C'est le sens des avis de la CNIL (19 mars 2015) et de la CNCDH (16 avril 2015).

[22] Pour W. Mastor (« La loi sur le renseignement du 25 juillet 2015. La France, État de surveillance ? », AJDA, n° 36, 2015, p. 2022), ces dispositions ne permettent pas la « surveillance » mais seulement la « collecte » de masse.

[23] Si, dans la décision du 4 août 2017, le Conseil avait censuré une disposition formulée selon lui en termes trop larges, la censure était cependant censée ne prendre effet qu'à partir du 1er novembre.

[24] Sont visées notamment par le texte les personnes « entrant en relation de manière habituelle avec des personnes ou des organisations terroristes ».

Certaines limites ont sans doute été posées par les juges : la CJUE a ainsi invalidé le 8 avril 2014 *(Digital Rights Ireland)* la directive de 2006 sur les données personnelles au motif que l'obligation de conservation de ces données imposée aux opérateurs constituerait une ingérence « d'une vaste ampleur » et « particulièrement grave » dans le droit au respect de la vie privée et, plus récemment, la législation suédoise de stockage des données (21 décembre 2016) ; quant au Conseil constitutionnel, il a censuré un article de la loi renseignement qui permettait au services de renseignement de procéder sans contrôle à la surveillance des communications par la voie hertzienne (21 octobre 2016)[25] et remis, plus généralement, en cause le droit l'accès des agents de l'AMF aux données de connexion (21 juillet 2017). Néanmoins, ces limites restent insuffisantes pour contrebalancer le mouvement qui pousse dans tous les pays à étendre la surveillance des communications électroniques.

L'essor des technologies numériques a donc permis le renforcement des dispositifs de surveillance, au risque d'alimenter le fantasme d'un *Big Brother* étatique contrôlant tous les mouvements du corps social. Si le fragile équilibre entre le respect de la vie privée et la protection de la sécurité collective se trouve modifié, la logique de surveillance rencontre cependant certaines limites structurelles ; l'exploitation intensive des données personnelles comporte d'autres risques au regard de la protection de la vie privée.

II. LA NUMÉRISATION COMME VECTEUR DE CONTRÔLE

L'idée d'une société placée sous la surveillance d'un État tout puissant, disposant par l'accès aux données personnelles d'une connaissance intime des individus et contrôlant leurs faits et gestes est illusoire. L'impact des technologies numériques sur la vie privée résulte avant tout de la collecte massive et de l'exploitation rigoureuse des données personnelles qu'elles autorisent : de vastes systèmes de données prolifèrent ainsi dans toutes les sphères de la vie sociale, réduisant d'autant la marge d'autonomie individuelle ; dépossédés d'éléments qui sont au cœur même de leur identité, les individus se trouvent exposés à un traçage numérique, en vue de cerner leur profil, définir leurs préférences et anticiper leurs comportements. Rassemblées dans des bases de plus en plus larges (A), les données font l'objet d'un traitement effectué par le moyen d'algorithmes (B).

A) L'essor des Big data

Impliquant la mise en relation et le croisement de masses considérables de données numérisées, recueillies à partir de supports divers et en fonction de logiques différentes, l'essor des *Big data*[26] comporte des risques évidents d'atteinte à la vie privée. Ces données sont de nature extrêmement diverse.

1° Les données publiques apportent une importante contribution à cette collecte, via les principes d' « ouverture par défaut » et de « réutilisation » qui, progressivement posés[27], constituent « l'axe fort »[28] de la loi sur la République numérique : l'institution par ce texte d'un « service public de la donnée », dont la mission est de mettre à la disposition de tous des « données de référence », en vue de faciliter leur réutilisation, ainsi que l'élargissement de

[25] Le Conseil donnait au législateur jusqu'au 31 décembre 2017 pour l'élaboration d'un nouveau texte, ce qui sera fait par la loi du 30 octobre 2017.

[26] Les *Big data* seraient caractérisés, non seulement par le Volume, la Vélocité et la Variété des données recueillie, mais encore par leur Véracité (données précises et exactes), leur Visualisation et leur Valorisation (attachée à l'usage).

[27] J. Chevallier, « Le droit français et la question des données publiques », in D. Bourcier et P. De Filippi, *Open data et Big data. Nouveaux défis pour la vie privée*, Mare et Martin, 2016, pp. 35 sq.

[28] L. Cluzel-Métayer, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », AJDA, n° 6, 2017, p. 342

l'*Open data* aux « données d'intérêt général », pouvant être considérées comme des données stratégiques, témoigne de nouvelles avancées en matière de « circulation des données publiques ». Les résistances opposées par certaines administrations à la réutilisation gratuite de leurs données sont en passe d'être levées, les redevances étant vouées à devenir exceptionnelles (décret du 20 novembre 2016). Tout se passe comme si l'État était appelé à devenir un « État-plateforme », chargé de mettre à la disposition du public un ensemble d'informations permettant le développement de services[29].

Cette ouverture n'est pas sans incidence sur la question des données personnelles : les données détenues par les administrations ayant été souvent élaborées à partir d'informations recueillies sur des individus, comme en matière de santé, les exigences de consentement et d'anonymisation risquent d'être tournées ; si l'ouverture des données publiques doit être poursuivie, il conviendrait ainsi, selon le Conseil d'État, de « prévenir les risques pour la vie privée », en définissant de « bonnes pratiques d'anonymisation », en vue de « limiter les risques de ré-identification »[30].

2° Tirant parti de cette ouverture des données publiques, les *Big data* sont alimentées par les possibilités toujours plus étendues de collecte de données personnelles offertes par les technologies numériques. Ces données sont recueillies de manière automatique, à partir des empreintes numériques laissées par les individus. Le recours à Internet pour tous les actes de la vie quotidienne, via ordinateurs, smartphones ou tablettes, contribue à fournir des informations de toute nature sur les comportements, les goûts, les opinions des intéressés ; les faits et gestes peuvent être suivis, la personnalité appréhendée, à partir des multiples traces décelables sur Internet. Ces traces sont fournies aussi par des capteurs intégrés au sein d'objets de la vie quotidienne (cartes bancaires, appareils électroménagers, titres de transport, passes autoroutiers, compteurs électriques[31]…), voire portés sur soi en tant qu'instruments de mesure, tous ces « objets connectés » étant appelés à connaître un développement exponentiel. Les données personnelles sont encore collectées indirectement, à travers les informations fournies par des tiers *(data shadows*).

L'idée de « données personnelles » semble dès lors avoir perdu une bonne part de sa signification et de sa portée : non seulement toutes ces informations sont recueillies avec le consentement tacite des individus qui ne voient que des avantages dans les facilités offertes par ces outils, mais encore les internautes n'hésitent pas à mettre eux-mêmes en ligne, via Facebook ou Twitter, un ensemble d'éléments touchant à leur vie privée, voire à leur intimité. D'énormes masses de données personnelles sont ainsi collectées par des grandes entreprises du Net, stockées dans des bases de données et traitées en vue d'une exploitation systématique, dans le cadre de ce qui est devenu un marché mondial des données, dominé par les GAFA (Google, Apple, Facebook, Amazon), principaux acteurs de l'économie numérique. Le transfert de ces données d'une continent à l'autre apparaît comme un enjeu économique essentiel : l'accord *Safe Harbor*, approuvé le 26 juillet 2000 par la Commission européenne, permettait ainsi aux entreprises américaines de transférer vers les Etats-Unis les données des Européens utilisant leurs services : la Cour de Justice de l'Union européenne ayant le 6 octobre 2015 invalidé la décision de la Commission, en constatant que les Etats-Unis n'assuraient pas un nouveau de protection adéquat, un nouvel accord *Privacy Shield* a été signé le 8 février 2016, entré en vigueur le 8 juillet[32]. Avec le développement des *Big data*, on

---

[29] Etude du Conseil d'État 2017 précitée, pp. 102-104.

[30] Rapport, préc., p. 309. Dans le même sens, G. Gorce, F. Pillet, *L'Open data et la protection de la vie privée*, Rapport d'information, Sénat, n° 469, 16 avril 2014.

[31] Sur le compteur Linky, voir C. Menard et C.J-B. Morel, « Le déploiement des compteurs communicants Linky », RFDA, n° 3, 2017, pp. 437-444.

[32] L'*Executive order* du nouveau Président américain en date du 25 janvier 2017 tend cependant à remettre en cause les garanties nouvelles données aux Européens.

tend vers une traçabilité intégrale[33] dans laquelle, l'individu étant cerné par les multiples traces de con activité, la notion de vie privée n'a plus guère de consistance.

Face à ce danger, une réaction s'est produite, notamment au niveau européen. Les deux arrêt de la CJUE de 2014, *Digital Rights Ireland* du 8 avril, invalidant la directive de 2006 sur la conservation des données, et *Google Spain* du 13 mai, reconnaissant un « droit à l'oubli » aux utilisateurs d'un moteur de recherche, ont constitué à cet égard une étape importante ; les juridictions nationales ont emboîté le pas[34]. Plus généralement, le nouveau règlement du 27 avril 2016 contient un ensemble de dispositions visant à une meilleure protection des données personnelles : exigence d'un consentement « explicite » et « positif » des individus sur la collecte d leurs données ; consécration du « droit à l'oubli », la personne concernée ayant le droit d'obtenir du responsable du traitement « l'effacement » dans les meilleurs délais des données à caractère personnel la concernant ; principes de « protection des données dès la conception » et de sécurisation par défaut », s'imposant à toute la chaîne de ceux qui manipulent des données personnelles, des collecteurs, *data brokers* aux GAFA. Dans l'attente de la transposition de ce règlement, la loi du 7 octobre 2016, au-delà du rappel des principes de neutralité, loyauté, transparence et de la consécration du « droit à l'oubli », a solennellement affirmé le droit pour toute personne « de décider et de contrôler les usages qui sont faits de données à caractère personnel la concernant » (art. 54)[35]. Parallèlement, la condamnation le 17 mai 2017 par la CNIL de Facebook pour atteinte à la vie privée, en raison de la « combinaison potentiellement illimitée de toutes les données des utilisateurs », manifeste une volonté nouvelle de s'attaquer aux dérives des géants du Net. Ces garanties nouvelles ne sont pas négligeables ; elles restent cependant d'importance limitée au regard du mouvement de fond qui tend à la publicisation des données personnelles.

Les conditions de traitement de ces données posent par ailleurs un problème de fond.

B) La gouvernance algorithmique

L'analyse de ces masses de données hétérogènes passe par le recours à des procédés de *data mining* permettant d'opérer les croisements et corrélations nécessaires en vue d'extraire les informations pertinentes au regard des finalités poursuivies : cette analyse est opérée par le biais d'algorithmes sophistiqués, visant à permettre une exploitation rigoureuse des données[36].

La technique est d'abord utilisée en vue d'optimiser le fonctionnement des services, afin de répondre mieux aux attentes des usagers, dans les domaines les plus variés (commerce, transport, santé…) : elle conduit à modeler les produits offerts et le prestations fournies en fonction des profils identifiés. Les algorithmes peuvent aussi avoir une finalité prévisionnelle et prédictive, en s'efforçant, par la définition de profils-type, d'anticiper les comportements qu'adopteront les individus : un large usage est fait de ce type d'algorithmes pour prévenir les attentats terroristes, et aussi, plus récemment, en matière de police ; la *Predictive Policing* a pour ambition d'aller au-delà de la prévention policière classique pour tenter de prévenir, à partir du traitement d'un ensemble de données statistiques relatives au phénomène criminel, une infraction[37]. Les algorithmes peuvent enfin servir d'outils décisionnels, en réduisant la part d'incertitude, d'imprévisibilité et de subjectivité qui s'attache à la prise des décisions :

---

[33] A. Mattelart, « Gouverner par la trace », *Mouvements*, 2010.

[34] Sur l'existence d'un droit au « déréfencement », voir C.E., 24 février 2017, Mme Chupin et autres, RFDA, n° 3, 2017, pp. 535 sq. , avec les conclusion Bretonneau.

[35] L. Cluzel-Métayer, préc., pp. 346 sq.

[36] P. De Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère du *Big data* », in D. Bourcier, P. De Filippi, *op. cit.* pp. 99-128.

[37] C. Piotrowicz, « Approche criminologique de la *Predictive Policing* en matière de sécurité intérieure : vers une prévention prédictive ? », in M. Touillier, dir.), op.cit. pp. 163-191.

leur utilisation par les décideurs publics et les services administratifs soulève d'importants problèmes, comme l'a montré le système d' « admission post-bac » ; la loi du 7 octobre 2016 indique que lorsqu'une décision individuelle est prise sur le fondement d'un traitement algorithmique, l'intéressé soit en être informé, « les règles définissant le traitement ainsi que les principales caractéristiques de cette mise en œuvre » lui étant, à sa demande communiquées (art. 4), le décret du 14 mars 2017 précisant les conditions d'application du droit d'accès à ces règles.

L'omniprésence des algorithmes, qui envahissent toute la vie sociale, ne peut manquer de réduire la marge de liberté individuelle : enfermant les individus dans une identité prédéfinie à partir des traces numériques qu'ils laissent, ils les assigneraient « à la reproduction automatique de la société et d'eux-mêmes »[38] : on serait par là en présence d'un contrôle social plus poussé et plus intrusif sur les comportements, le prédictif glissant au prescriptif, en tendant à la normalisation des conduites. Un cyber-contrôle, d'autant plus efficace qu'il est invisible et automatique, puisque fonctionnant sur la base d'algorithmes de traitement des données laissées sur le Net, tend à se substituer aux procédés traditionnels de contrôle. Reposant sur « une confiance abusive dans les résultats d'algorithmes perçus comme objectifs et infaillibles »[39], la gouvernance algorithmique n'est qu'une nouvelle version de la « gouvernance par les nombres »[40], reposant sur le chiffre et le calcul : « le raisonnement aléatoire disparaît progressivement au profit d'une vérité numérique fabriquée à partir des données personnelles »[41] ; le souci de mieux encadrer leur utilisation, à travers des garanties de procédure et de transparence[42] ne saurait suffire à freiner le recours à une technique qui doit trouver dans l'intelligence artificielle un nouvel appui.

S'il confère à certaines libertés individuelles une portée nouvelle, l'essor des technologies numériques est ainsi lourd de menaces pour la vie privée : les possibilités inédites de surveillance qu'elles offrent modifie l'équilibre entre liberté et sécurité ; et la diffusion des données personnelles qu'elles entraînent réduit la marge d'autonomie individuelle. La prise de conscience de ces menaces a conduit, au terme d'initiatives convergents, prises tant au niveau européen qu'au niveau national, à un renforcement des systèmes de protection existants ; néanmoins, quelle que soit leur importance, les dispositifs juridiques ne sauraient suffire à endiguer une dynamique qui renvoie à une transformation d'ordre plus général ; l'inflexion de la conception traditionnelle de la vie privée n'est en effet qu'un des aspects des bouleversements de tous ordres induits par une révolution numérique qui atteint tous les éléments constitutifs de l'ordre social.

---

[38] Dominique Cardon, *A quoi rêvent les algorithmes ?. Nos vies à l'heure des big data*, Seuil, La République des idées, 2015.

[39] Conseil d'État, préc., pp. 234-235.

[40] Alain Supiot, *La gouvernance par les nombres,* Fayard, 2015.

[41] M. Dugain, C. Labbé, *op. cit.* p. 8.

[42] Voir le lancement le 23 janvier 2017 par la CNIL d'un débat public sur les algorithmes.